IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 September 2023, accepted 25 September 2023, date of publication 29 September 2023,
date of current version 4 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3320945

SURVEY

Exploring Trust Modeling and Management Techniques in the Context of Distributed Wireless Networks: A Literature Review

TERI LENARD[1,2], **ANASTASIJA COLLEN**[1], **MERIEM BENYAHYA**[1], **NIELS ALEXANDER NIJDAM**[1], **AND BÉLA GENGE**[3]

[1]Centre Universitaire d'Informatique, Geneva School of Economics and Management, University of Geneva, 1227 Carouge, Switzerland
[2]The Doctoral School of Letters, Humanities and Applied Sciences, George Emil Palade University of Medicine, Pharmacy, Science, and Technology of Târgu Mureş, 540139 Târgu Mureş, Romania
[3]Department of Electrical Engineering and Information Technology, Faculty of Engineering and Information Technology, George Emil Palade University of Medicine, Pharmacy, Science, and Technology of Târgu Mureş, 540139 Târgu Mureş, Romania

Corresponding author: Teri Lenard (teri.lenard@unige.ch)

This work is supported by the OPEVA project that has received funding within the Key Digital Technologies Joint Undertaking (KDT JU) from the European Union's Horizon Europe Programme under grant agreement No 101097267 and was co-funded by the Swiss State Secretariat for Education, Research and Innovation (SERI) and the Innosuisse—Swiss Innovation Agency. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or KDT JU. Neither the European Union nor the granting authority can be held responsible for them.

ABSTRACT Trust Modelling and Management (TMM) techniques are frequently applied in ad-hoc Distributed Wireless Networks (DWNs) to stimulate and improve cooperation between network nodes. TMM facilitate DWNs in building a trust network that assures reliability of communication channels, offers an additional layer of security, and enables group decision making processes. Likewise, TMM became in the past decades an attractive solution for solving problems in cooperative ad hoc DWN. The proposed solutions focus on modelling trust in a social-centric approach to maintain a system where nodes trust each other, and detect untrustworthy (malicious) neighbours. The work at hand considers a time span of three years, from 2020 to 2022, where the scientific research in the domain of TMM and DWN is analysed. Our survey aggregates over 130 research papers and investigates the quality of experimental assessment done by each work. Additionally, we establish an indication on the level of experimental analysis done by each study from a TMM security perspective. Lastly, the survey offers a trust ontology, a general overview of a trust models, together with a concise description of trust threats to facilitate the reader's understanding of TMM.

INDEX TERMS Trust modeling and management, distributed wireless networks, ad-hoc networks.

I. INTRODUCTION

The communication system called DWN creates a bridge between networking domains, such as Internet of Things (IoT), Wireless Ad Hoc Networks (WANETs) and Vehicular Ad Hoc Networks (VANETs), which links together common features scattered from each research domain. DWNs can be implemented as ad hoc, implying the lack of a static infrastructure, in comparison to traditional networking systems, where the topology is known. Particularly, nodes can spontaneously join and leave the network and act as consumers and servers. Message exchanges happen in a peer-to-peer fashion [1], which allows these systems to be self-governing. Likewise, each network's member is responsible for forwarding and routing packets, offering access to network services, and participating in group decision making processes [2].

DWNs are considered more prone to cyber threats and attacks, due to their ad hoc nature [3]. In general, malicious actors can eavesdrop on wireless communication channels to intercept and alter packets on the fly, mimic legitimate network nodes in systems where strong encryption is not present, and target encryption and authentication protocols to exploit improper security practices [4]. In collaborative DWNs, malicious actors have a different attack scope. Instead of conducting a disruptive cyber attack in the

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

traditional sense (e.g., denial of service), their intention is to maintain persistence over a longer period of time. The replication of normal networking behaviour is meant to disrupt collaborative processes at a later time (e.g., group decision and election processes) [5].

The aforementioned security concerns, combined with the intrinsic properties of DWNs, pushed academic researchers towards TMM. TMM employs scientific and technical methods as a means to solve particular problems that involve trust relationships to be maintained over long periods of time [6]. Due to its similarity with social networks, from where trust modelling originates [7], both, include a set of *agents*. From this set, an agent, called *node*, communicates only with a subset of nodes. Moreover, nodes are required to exchange trustworthy information among them to facilitate the group's well-being. In contrast, malevolent agents, representing malicious network nodes, should be excluded from the group through denying the right to participate in group decisions and information sharing.

TMM stimulates and improves cooperation between network nodes as well as assures a reliable communication environment which guarantees an additional layer of security on top of the existing communication channels. A trustworthy relationship is established between a network node, known as a *trustor*, and other nodes known as *trustees*. The relationship is considered *trustworthy* by a trustor, if the trustee can accomplish a specific task given by the trustor [8]. Trust modelling shapes how trust evolves in a group composed of multiple trustors and trustees, based on a series of current and past observations (trust metrics), to obtain levels of trustworthiness [7]. Trust management, on the other hand, focuses on collecting the necessary observations that are required to establish trustworthy relationships. Additionally, trust management must dynamically monitor and manage trust relationships [9].

TMM is capable of building a dynamic trust network, where the interactions between nodes establish trust relationships. Moreover, TMM facilitates group formations, distributed decision making aimed at preserving the network security, and lastly, network behaviour monitoring and modelling. From a security perspective, TMM must be resilient against potential threats, which are a combination of traditional cyber attacks and a social-behavioural malevolent demeanour. In a TMM setting, a malicious actor may act genuinely for a period of time, obtaining as consequence a high level of trust, only to have dishonest behaviour later [10]. This scenario becomes more complex when malicious nodes are acting harmfully with everyone, publishing false trust advertisements, intentionally discriminating certain nodes to limit access to their services, or alternating their benevolent and malevolent behaviour to conduct attacks over longer periods of time [11]. The robustness of the TMM eventually should be measured based on the resistance against such attacks.

Our motivation relies on the significant amount of research papers published in the field of TMM, making it of crucial importance to systematise and review the acquired academic knowledge. Multiple previous works [6], [7], [12], [13] already paved the road for a better understanding of how trust is measured, modelled and managed in complex DWNs. Consequently, the present work aims to explore and expand this effort through the following contributions:

(i) *Ontology*: Provides clarity on TMM terminology by building a trust ontology, defining a generic trust model, and identifying the most noteworthy trust threats.

(ii) *Survey*: Identifies, outlines and analyses the most relevant studies targeting TMM in DWNs in the past 3 years (from 2020 to 2022) by following a Review Protocol (RP).

(iii) *Analysis*: Investigates and compares research studies by assessing three indexes: evaluation, validation and threat resistance.

The remainder of the paper is structured as follows. In Section II, we provide background information regarding DWN. Section III outlines the relevant related works. In Section IV, TMM concepts are introduced, together with trust model ontology, and the potential trust threats. Afterwards, our research methodology is outlined in Section V, continuing with the comparison and analysis in Section VI. The paper wraps up with a discussion in Section VII, and the open research gaps in Section VIII. Finally, the paper concludes in Section IX.

II. BACKGROUND

DWNs encompass communication systems which contain multiple wireless devices that collaborate to maintain the system's infrastructure. Devices or nodes often communicate in a peer-to-peer fashion, forwarding and routing packets, offering network service access to other devices and users, and participate in group related tasks. Examples of DWN range from IoT systems, to Wireless Sensor Networks (WSN), ad hoc networks, WANET or newer technologies like VANET, to mention a few.

In the context of DWN, IoT represents heterogeneous communication systems, composed of embedded devices that leverage sensors to capture information on their surrounding environments [14]. What makes this system *smart* is the fact that the information captured from the sensors is meant for processing to achieve better system automation, decision making and monitoring. The applicability of IoT in real life environments range from smart cities [15], industrial sector [16], environment and agriculture monitoring [17], transportation [18], or home automation [19].

Compared to IoT which includes feature rich sensing devices, WSN incorporate a large number (in the order of tens or hundreds) of computational restricted devices spread across a large environmental area (e.g., forest) [20]. In both, IoT and WSN, the end devices are tasked with collecting environment data (e.g., humidity, temperature, light, movement) which is usually aggregated and further processed by one or multiple central gateway units. On its turn, a gateway handles the necessary communication with external cloud services which can help in complex data analysis and visualisation.

A key distinction between IoT and WSN is that the devices in the latter system, must be capable of self-organisation in groups (i.e., clusters), require cooperation in task handling, and need to function with minimum human interaction [20]. Tolerance to faults and system availability represent as well key features that must be exhibited by WSN. Even if devices break, or run out of battery, the system must function. This brings up the ad hoc aspect into discussion, and the relation between WSN and WANET. The ad hoc element allows devices to spontaneously join or leave the system (i.e., or group) while maintaining in parallel the system's normal functioning state [3].

The ad hoc feature is embraced even more, when device mobility represents a core system requirement. This is highlighted by DWN such as Mobile Ad Hoc Network (MANET) and VANET. In these wireless systems, devices are free to move across a geographic area, the mobility factor making the network infrastructure more dynamic in terms of changes, as nodes leave and join groups more frequently [21].

While the section at hand intends to provide a high level overview of different types of DWN, together with their key characteristics and relationships, the benefit that TMM approaches can bring up is clear as system requirements become more complex. TMM can aid DWN in establishing trustworthy relationships between devices which can contribute to improved and more reliable communication (i.e., in case of routing), establish trustworthy group leaders (i.e., in case of clustering), and selecting the best communication neighbour with a low chance of establishing communication with a malicious node.

III. RELATED WORK

The related work at hand compiles a succinct overview of the most notable surveys targeting TMM and DWNs. Related works are outlined in a chronological order to clearly display the progress achieved in the literature. To offer a better overview regarding TMM methods, we cover a broader range of DWNs (e.g., IoT, WSN, MANET) where TMM is applicable. Ultimately, the scope of the review is to inspire and offer the reader an overview as broad as possible regarding TMM in DWNs.

The authors of one of the earliest works found [7], elaborated a literature review of trust modelling methods in the context of ad hoc networks. Their research demonstrated a qualitative comparison between different modelling approaches which were implemented in various domains (e.g., information or game theory, clustering).

Gómez Mármol and Martínez Pérez [13] brought attention to several problems present in the literature. Their motivation lied in the problematic of studies focusing mostly on the descriptions of the implemented methods, while sufficient experimental results to demonstrate the accuracy of the approaches still lacked. For a better understanding of the accuracy and plausibility of trust models, the authors developed a specially tailored simulation tool named TRM-Sim, which permitted the authors to implement several models to measure and compare their effectiveness and performance under different conditions targeting close to reality environments.

Afterwards, Cho et al. [5] put together a clear list of attacks targeting TMM in MANET. Additionally, the authors outlined an in-depth analysis of proposed TMM for MANET, as well as a comprehensive set of definitions in the context of MANET that usually were found in different TMM contexts (e.g., Sociology, Economy). Cho continued her work in [6], pointing out the difficulty to obtain clear and quantifiable trust metrics due to the diverse nature of TMM application domains. Furthermore, the survey aimed to present clear and concise definitions regarding trust, offering a foundation on how to apply trust at different layers in a complex network. On the same note, Guo et al. [24] leveraged further the trust categories defined by Cho et al. [5] to analyse and categorise service oriented IoT TMM. Similarly, Amin et al. [25] offered a brief literature analysis in which problems regarding scalability, adaptability and network structure are discussed from the point of view of TMM in IoT.

The survey of Sharma et al. [27] stands out compared to other works, as they explicitly mention for each analysed study, the input trust metrics together with the performance metrics used to validate the models. Likewise, Chahal et al. [28] presented relevant knowledge on trust metrics with an additional classification and comparison of TMM's methods based on their applicability, computational model, model inputs, evaluation tool and performance metrics.

In Wireless Body Area Network (WBAN), Ayed et al. [29] emphasised on best practices that pinpoint key elements for building a TMM, besides providing a literature analysis. Siddiqui et al. [30] focused on the state of the art of VANET TMM. The authors summarised attacks and threats on TMM, categorised most relevant works based on their approach (e.g., traditional, Bayesian inference, fuzzy, machine learning and Blockchain), and pointed out several gaps deduced from the literature survey. The conclusion is that most works do not answer the problems of threshold computation, cold start, data scarcity or weight quantification. Similarly, Ahmed et al. [26] presented the trust terminology under the umbrella of IoT, together with trust-based studies and trust related attacks.

More recently, Marche et al. [11] tried to answer the question if TMM can be trusted, by performing an experimental assessment in a simulation environment using the "IoT/SIoT" dataset [32] with various trust models. In the same year, Mannix et al. [31] outlined a comprehensive survey on WSN, where a high-level trust model structure was presented, with an analysis of trust attacks types, and a thorough presentation of trust parameters and metrics used in the literature. Additionally, older studies [26], [30] considered that trust models keep leveraging static

TABLE 1. Comparison between the most note-worthy literature surveys targeting TMM and present work. (✓- considered, ✗- not considered, ∼ - partially considered.)

Source	Year	Domain	Review type	Trust concepts	Trust threats	Trust metrics	Evaluation
[7]	2009	Ad hoc networks	Scoping	✓	✗	∼	Qualitative
[13]	2011	DWN	Scoping	∼	∼	∼	Comparative Simulation
[5]	2011	WANET	Traditional	✓	✓	✓	Comparative
[23]	2014	DWN	Scoping	✓	✓	∼	Comparative
[24]	2014	IoT	Scoping	✓	✗	✗	Comparative
[6]	2015	N/A	Traditional	✓	✗	✓	Qualitative
[25]	2017	IoT	Scoping	✓	✓	✗	Comparative
[26]	2019	IoT	Scoping	✓	✗	✗	Comparative
[27]	2019	IoT	Scoping	✓	✓	✓	Comparative
[28]	2020	IoT	Scoping	✓	∼	✓	Comparative
[29]	2020	IoT	Scoping	✓	✓	✓	Comparative
[30]	2020	WBAN	Scoping	✓	✓	✓	Comparative
[12]	2020	DWN	Scoping	✓	✓	✓	Comparative Experiments
[31]	2021	VANET	Scoping	✓	✓	✓	Comparative
[32]	2022	WSN	Scoping	✓	✓	✓	Comparative
[11]	2022	IoT	Systematic	✓	✓	∼	Comparative Experiments
Our work	2023	DWN	Systematic	✓	✓	✗	Quantitative Comparative

thresholds instead of dynamic ones in the model decision making.

Following this analysis, it can be concluded that the field of TMM matured in time, has clear definitions and terminology [5], [6], [33], methods and algorithms [28], [29], [30], [31], and scope in terms of trust collaboration, threats and threat models [11], [12], [26], [30]. Additionally, a pattern frequently observed after breaking down the studies in chronological order, is that the same open issues and gaps are still found and mentioned, ranging from the generality of the model, to experimental validation, to thresholds and weights computation.

To support in solving the gaps, the survey at hand aids in the following manner. To push towards model generality, our survey offers a trust ontology and a concise outline of a trust model. Additionally, our study identifies the most frequently addressed trust threats/attacks. The motivation relies on the need for a deep assessment of the quality of work from the perspective of the model experimental validation in the presence of trust threats. Lastly, a comparison between the works presented in this section is given in Table 1. Here, the surveys analysed are presented in chronological order, summarising the research domain covered (3rd column), type of review (4th column), key trust notions addressed (5th to 7th column), and the type of evaluation conducted (8th column). Based on our findings, along Marche et al. [11], the present work is one of the few literature surveys in the the domain of TMM targeting DWN with a systematic approach. The added value of our work relies in replicability of our research, as it allows researchers to follow the steps and review protocol considered, to reproduce, verify, and extend the present findings.

IV. TRUST CONCEPTS AND ONTOLOGY

Designing a comprehensive TMM method and understanding its intrinsic properties implies three distinct, yet inter-related pillars. Pillar one (P-I) supports the fundamental concepts, definitions and terminology surrounding TMM. The second pillar (P-II) builds on top of the P-I to establish the most significant parts which construct a TMM. Lastly, the third pillar (P-III) addresses the utility of TMM methods when faced with trust related threats. This foundation is formalised in the work at hand by building a trust ontology to support P-I, presenting the fundamental blocks of a trust model for P-II, and, lastly, identifying the most frequently mentioned trust threats in the literature for P-III.

A. P-I: TRUST ONTOLOGY

The scope of an ontology is to provide a structure that defines, analyses, extends and shares domain knowledge [34]. Through a trust ontology, trust concepts together with their relationships are hierarchically arranged. This structured approach is meant to aid the reader in understanding the terminology leveraged and the background knowledge relevant to TMM.

The scientific literature offers a diverse palette of trust ontologies. For example, an automated trust negotiation ontology-based method was formalised using a description logic by Liu et al. [35]. To highlight semantic relationships between nodes and heterogeneous data, authors of [36] outlined a trust model targeting sensors in pervasive environments using an ontology. Similarly, Taherian et al. [37] constructed an ontology to model trust in a similar ecosystem. Through multiple works, [22], [33] a simple trust ontology was defined with a common formal semantic to better describe a comparative analysis of distributed trust models that employ Bayesian approaches. Particularly, the authors' analysis asserted that TMM seems similar at the first glance, but contain subtleties that differentiate themselves in non-trivial ways. Additionally, there are trust ontologies focused on other domains than DWNs, such as Information Services [38], Service Semantics [39] or Cloud Services [40], as well as more general approaches [41], [42], [43], [44] that still have TMM as a focus.

Our ontology expands upon the insights offered by Sharma et al. [27] and Siddiqui et al. [30] in terms of trust definitions, and the ontology proposed by Thirunarayan et al. [22]. By gathering this knowledge under a singular frame, the trust ontology presented in Figure 1 emerged. Accordingly, four main blocks were identified:

(i) *Trust relationship*: reflects the actual relationship established between a trustor and trustee(s).

(ii) *Trust aggregation*: presents how multiple trust values, obtained directly or indirectly from peers, are combined under a unique value [29].

(iii) *Trust update*: defines the process used to compute the next trust values [26].

(iv) *Trust propagation*: outlines the process to exchange and publish trust information across the network [26].

The *trust relationship* (i) is subjective in nature, held by a *trustor* on one or more *trustees*. The relationship can be established in two ways. On one hand, if the trustor interacts directly with a trustee, the relationship produces *direct trust*. Otherwise, if the trustor does not interact directly with a trustee, the trustor can obtain trust values from its neighbourhood and consider that as *indirect trust* (e.g., recommended trust). The subjectivity aspect of a trust relationship, and the uncertainty the trustor manifests when assessing its trust was also pointed out by known works on trust [6], [45], [46], [47], [48]. Those works further argue that there is a risk that must be considered by the trustor when it entrusts a trustee to exhibit a behaviour.

Trust aggregation (ii) or trust computation refers to the concrete model leveraged to compute trust values. It utilises a set of input parameters or attributes, named trust metrics, to compute trust values. In accordance with Thirunarayan et al. [22], trust aggregation, computation, or process, can be *reputation-based*, *policy-based* or *evidence-based*. Methods based on reputation consider past behaviour over time, the policy focused ones are restricted to specific constraints for decision making, and the evidence-based ones demonstrate proofs for evidence.

Trust update (iii) plays the role in triggering the process which computes new trust values. This involves new observations (e.g., trust metrics) to compute direct trust, and trust recommendations for indirect trust. The conditions in which this happens may be event-driven, trust information being propagated only when a specific event takes place, or periodical, when the scheme is time-driven [29].

According to [24] and [29], *trust propagation* (iv) can be of two types: centralised and distributed. Centralised approaches require trusted entities (e.g., centralised network members) responsible to propagate the information into the network. Conversely, distributed trust propagation happens autonomously where each network node contributes to the propagation process. This involves operations such as trust composition, prediction, and formation. The composition aspect of trust implies a procedure to combine social related metrics with other sources of trust metrics [26]. The process of predicting the next trust value is often used in TMM, especially in Bayesian oriented approaches, as an intermediate step to validate a trust value propagated from a trustee. Finally, trust formation is dedicated to combining multiple trust metrics computed from distinct sources under a single value.

B. P-II: TRUST MODELLING

Understanding the building blocks of a trust model is a first step in a model design. By leveraging the aforementioned trust ontology, a high-level overview of a trust model is defined. Consequently, four blocks were considered to cover the functionalities of a trust model: (i) input, (ii) storage, (iii) computation and (iv) output.

The model *input* consists of two sources of trust metrics obtained via the trust propagation process. The first source represents external input measurements or trust metrics used by the trustor for direct trust computation. The second input represents trust recommendation (e.g., indirect trust) received from neighbours. The computational model handles direct and indirect trust values to determine the trustworthiness of a node. The input trust metrics represent an essential element of the trust model. Based on the thorough analysis of the metrics from the state of the art, it can be stated that trust metrics depend on the computational model and on the environment in which the model runs. This implies that the model's input impacts its performance and reliability.

In terms of *storage*, a model maintains historical observations, composed of direct and indirect trust values, employed by the computational model. The intention to store and use past trust values over a predetermined time window is to emphasise the effect of past interactions into the future model's decisions. This further implies a discard procedure which forgets outdated trust values accumulated in the time window considered. Discarding trust values limits the amount of values taken into consideration in computing trust values.

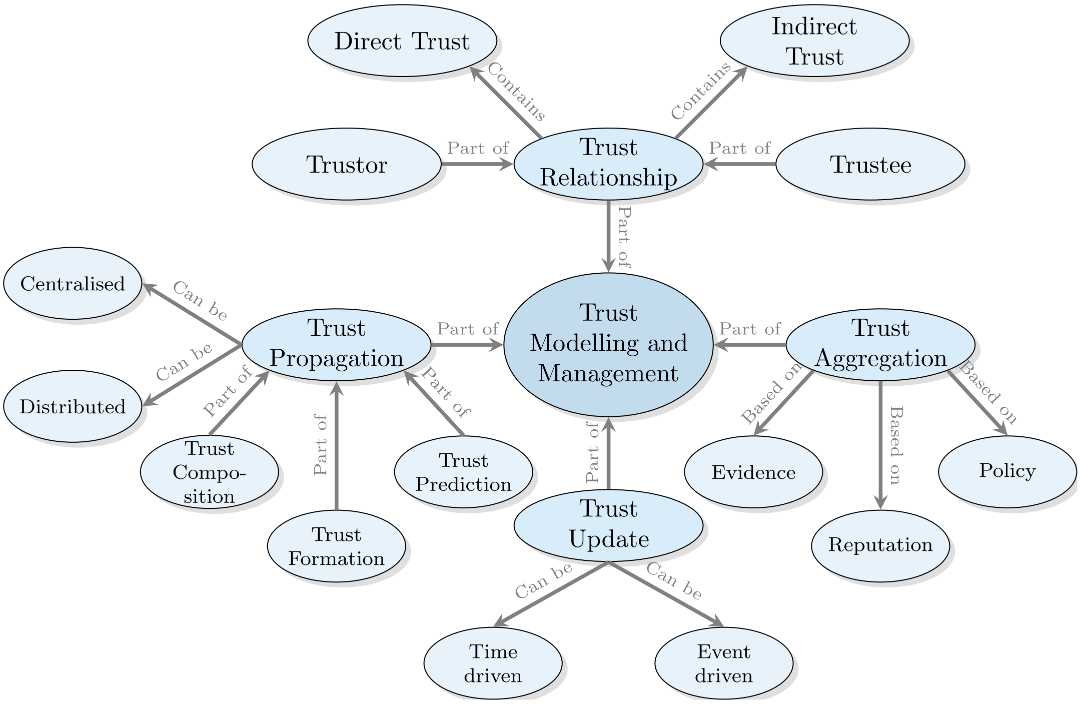

FIGURE 1. Trust ontology.

This limits the maximum storage space required by the model. On the same note, the time window will ultimately influence the model's decisions. A wide time window allows certain trust attacks (e.g., On-off), while a small time window offers insufficient trust information. An alternative to time windows is to have a trust aggregation function with the property to maintain the influence of a trust value at a given time step for the next time step.

The *computation* is required to compute direct trust by considering historical trust observations and trust metric. Secondly, indirect trust values are computed based on trust recommendations, direct trust, and historical observations. Once trust values are computed, the model propagates their current trust values for a specific neighbour to other models as recommendation. Lastly, a trust aggregation process takes a set of recommended trust values and a direct trust value to compute fused trust value about a specific node.

The fused trust value is leveraged by a trust model to generate the model *output*. The fused trust is compared against a decision threshold to determine if a node is trustworthy or not.

C. P-III: TRUST THREATS

TMM is ultimately a security mechanism designed to enforce reliable and trustful interactions within a group of nodes. Additionally, to the decision making mechanisms, TMM focuses on punishing uncooperative nodes (e.g., untrustful nodes) which tend to disturb the expected functional behaviour of the network. Consequently, it is essential for a TMM technique to be resilient against threats. Trust attacks merge aspects from traditional network-oriented attacks (e.g., Man-in-the-middle (MITM), spoofing, replay), with malevolent behaviour that individuals exert in social groups. By inspecting the literature [24], [26], [29], [30], [31], the following potential trust threats were identified:

- *MITM*: Interception and/or packet modification.
- *Sybil (SYB)*: Claiming/stealing multiple identities. Used for self-promoting, or biased/false advertisements.
- *On-Off (OO)*: Continuously switching between honest and dishonest behaviours. The attack is also known as traitor, zigzag or garnishing.
- *Selective behaviour (SB)*: Selective offering of services, discriminatory forwarding or packet dropping. Analogous to On-Off attacks.
- *Black-hole (BH)*: Positive self-advertisement to receive and drop packets, similar to a sinkhole.
- *Bad-mouthing (BM)*: Advertisement of fake trust/reputation information. Sometimes called Ballot-stuffing.
- *Collusion (CL)*: Malicious group advertises biased recommendations to increase their reputation and decrease legitimate ones.
- *White washing (WW)*: Rejoining the network/group with a new identity to *wash* past bad reputation. Also known as newcomer attack.
- *Impersonation (IMP)*: Stealing/cloning legitimate identities to behave maliciously. Also known as counterfeiting, spoofing or identify fraud.
- *Generic (GEN)*: Identifies as general malicious behaviour.

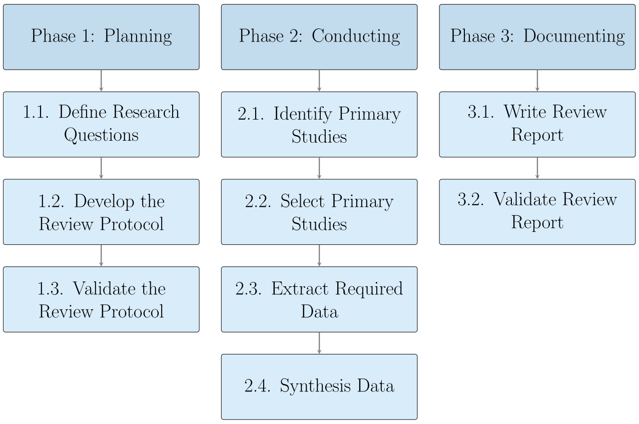
Phase 1: Planning
1.1. Define Research Questions
1.2. Develop the Review Protocol
1.3. Validate the Review Protocol
Phase 2: Conducting
2.1. Identify Primary Studies
2.2. Select Primary Studies
2.3. Extract Required Data
2.4. Synthesis Data
Phase 3: Documenting
3.1. Write Review Report
3.2. Validate Review Report

FIGURE 2. **Review process according to Brereton et al. [49].**

To conduct the attacks, the malicious actor must compromise a network node and gain control over it. The success of the attack depends on the attacker's capability to execute the same communication protocols, possibly over a secure channel, with other nodes in the network. Additionally, the malicious actor is required to gather information on the trust model executed in the network to actively influence other nodes' trust values. The goal for an attacker which intends to compromise a trust model, is to obtain high trust values in the long run to influence the group decision making processes, remain concealed to alter opinions on specific nodes, resulting in service disruption, or to forcefully isolate nodes through false advertisements.

Consequently, the survey at hand considers appropriate to give the security dimension of TMM a higher level of attention. Therefore, the trust threats identified in P-III are attributed within each study surveyed. Furthermore, the terminology of P-I and P-II is employed in the analysis of the surveyed works, presented in detail in Section VI.

V. RESEARCH METHODOLOGY

The core component of a Literature Review (LR) is the establishment of the RP. The present RP follows the recommendations and guidelines offered by Brereton et al. [49]. The authors proposed a three-phase methodology, outlining how to plan, design and conduct the LR. As illustrated in Figure 2, Phase 1 of the methodology consists of defining the Research Questions (RQs) intended to be answered by the survey, a RP that explains each step taken to conduct the research, and the procedure to validate the RP. In Phase 2, the RP is applied to identify, select and analyse research studies. Lastly, the research is documented and validated in Phase 3.

A. PHASE 1: PLANNING

The survey conducts a comparative analysis of TMM techniques published from 2020 to 2022 in the field of DWN. According to Brereton et al. [49], the RP outlines in depth the steps followed during the survey. The RP at hand, was defined and fine-tuned by all members of the review group (i.e., authors), to limit incorrectness occurrence during primary study analysis and data extraction. Here, the term *primary study* denotes the articles undergone the review. Moreover, by having all authors involved in the protocol design, a more uniform set of results can be obtained, and bias is limited. The first step in building the RP was to define the scope of the survey, by identifying the targeted RQs. Afterwards, the process of searching, selecting, and categorising research papers was formally defined. Lastly, the RP was validated internally by the review group individually as suggested in [49].

The RQs together with the motivation of the paper, as stated in the introduction of the survey, focus on the quality of experimental assessments, threat resistance and security, with an additional emphasis on identifying the core components and terminology of TMM.

RQ 1: What are the advantages, motivation, and objectives behind TMM?

RQ 2: What are the most frequently applied TMM methods?

RQ 3: What are the core components of a generic TMM technique?

RQ 4: What is the security validation degree undertaken by studies?

RQ 5: What are the security issues addressed by TMM in the domain of DWNs?

B. PHASE 2: CONDUCTING

Phase 2 aims to implement the execution of the RP previously defined. It is composed of the selection and exclusion process for primary studies from a set of databases, outlining the criteria for article inclusion in the review, and record the procedure for clear and reproducible results.

The selection of primary studies started with specifying a set of databases. Table 2 presents the sources used, side by side with the number of results obtained. For each database the advanced search option was used to obtain more accurate results. It is to note that databases, such as Google Scholar, were excluded from the search methodology since preliminary findings yielded a high number of duplicated primary studies that were already found in existing databases (e.g., IEEE Xplore, Science Direct). Consequently, the search methodology was restricted to scientific publishers' databases.

The first filter applied was to limit the publishing years of primary studies in the range from 2020 up to 2022. The second filter refers to the domain of activity, where the search was limited to primary studies related to DWN in the domain of Computer Science, excluding published papers in different areas (e.g., Social Networks, Economics). Furthermore, the last restriction filters out the article type, to limit the results only to research papers. Finally, the generic search query was defined as shown in Table 3.

The primary studies analysed were published under an *open-access* policy, or were accessed through research subscriptions offered by University of Geneva. Manuscripts

TABLE 2. Databases and query results.

Source Name	Link	First Query	Second Query	Selected	Excluded
Wiley Online Library	onlinelibrary.wiley.com/	1,998	964	14	1
ACM Digital Library	dl.acm.org/	11,053	327	13	10
Science Direct	sciencedirect.com/	9,956	1,486	82	17
IEEE Xplore	ieeexplore.ieee.org	9,483	6,311	137	103
MDPI	mdpi.com/	3,162	799	20	3
Emerald Insight	emerald.com/insight/	19,803	1,753	8	7
Total		55,455	11,640	274	141

TABLE 3. Search query.

('Wireless Networks') <and> ('trust modelling'
<or> 'trust management' <or> 'trust modelling and management'
<or> 'trusted framework' <or> trust <or> trustworthy)
<and> (year >= 2020 <and> year <= 2022)

not covered by the access policies mentioned were subjected to exclusion.

The query key terms were first searched in the primary article's title, key words, abstract, and content. This extended search procedure, while intended to find a higher number of primary studies, produced a high number of mismatches as seen in the *First Query* column of Table 2. To get more concrete queries, the search was limited to the primary study title and abstract. The corresponding results can be observed in the *Second Query* column of Table 2. Once the studies were identified and noted, the exclusion process began with screening the abstract and key words of the studies. Those that did not fit the survey scope together with duplicated ones were excluded. By limiting our search to databases of scientific publishers, and excluding scientific search engines (e.g., Google Scholar), a low number (approximately five) duplicated primary articles was found. Afterwards, the eligibility of the studies was assessed by reviewing the entire manuscript. Lastly, the scientific contributions of the primary studies were evaluated, and the last exclusion process took place. Finally, from 274 articles selected for the survey, 141 papers were excluded based on our RP, resulting in 133 research papers.

C. PHASE 3: DOCUMENTING

Preliminary to writing the review report resulting in the survey at hand, a template was defined based on which the documenting phase took place. Consequently, the studies were grouped according to the technique considered for TMM. Nine categories were considered to cover the vast range of papers on TMM. These categories range from modelling techniques (e.g., Bayesian inference and statistics, fuzzy theory, belief theory, subjective logic), to routing and clustering TMM, and Blockchain in several cases for trust management. Each category is outlined in Section VI individually and complies with the defined template by adopting the same formal structure for each subsection. First, for each category a brief introduction on the topic is given. Secondly, a succinct study overview outlines most relevant works and compares them. And thirdly, a table provides a complete summary of all categorised papers included in the survey, together with the comparison criteria attributed. Lastly, the review report resulted was formally analysed by each member of the review group. The feedback was gather from each member and assessed to improve the quality of the survey.

VI. COMPARISON AND ANALYSIS

Since TMM provides a layer of security on top of a distributed decision making technique, the authors considered essential to compare the research papers in the current survey from a security standpoint. Meaning that, besides providing an overview of the TMM functionality, the comparison focuses on pointing out the degree of experimentation undertaken in each paper, the threats considered in TMM design, and trust attacks considered in the validation process. Consequently, three distinct evaluation indexes were defined:

(i) *State-of-the-art Comparison Criteria (C1)*: As the name suggests, this criterion is concerned with the fact that the authors compared their proposed work with other relevant methods already available in the literature.

(ii) *Performance Analysis Comparison Criteria (C2)*: This index states what scope of experiments the authors provided to validate their proposed work, in terms of computation cost, or network performance.

(iii) *Threat Evaluation Comparison Criteria (C3)*: This index focuses on security evaluation the authors conducted to validate their work.

For these evaluation indexes, three distinct levels of completeness were defined: (i) *considered*, denoted by the check mark symbol (✓), (ii) *not considered* denoted by an x-mark (✗), and (iii) *partially considered* denoted by a tilde symbol ($\sim$). Here, partially considered denotes the fact that the index was not fully addressed, and there is not sufficient evidence to judge the completeness of the work.

Each of these levels of completeness are displayed in the tables associated with the categories considered in studies' grouping below. We highlight that in certain cases authors did not explicitly state trust attacks. Consequently, besides the mentioned trust attacks from Section IV, a *Generic* attack notion was utilised. This attack was used to cover the cases when authors discuss and conduct validation against trust attacks without offering sufficient details, symbolising a malicious behaviour without particularities.

A. BAYESIAN THEORY AND STATISTICAL MODELS

Bayesian Theory [78] represents the groundwork on top of which several generalised frameworks (e.g., Dempster-Shafer Theory (DST), Subjective Logic (SL)) were built upon. Additionally, as Table 4 depicts, a variety of trust models were researched. Known as well as Bayes' theorem, Bayesian Theory offers a mathematical foundation for calculating probabilities with uncertain information. Bayesian Theory expresses prior probabilities as a belief about the likelihood of a given hypothesis. Posterior probabilities represent the outcome of an updated prior probability once new observations become available, expressing the new belief about the hypothesis based on the new observations. Bayesian inference is introduced as a process meant to update beliefs on a given hypothesis when new observations are available. The inference process is accomplished by computing posterior probabilities for each given hypothesis based on the observation available and the prior probability, resulting in a prediction conditioned by past events. These elements can be brought together under the form of a Bayesian network, to express under the form of a graph, or network, the probabilistic relationships between entities. Being closely related, statistical models on the other hand, leverages statistical analysis, binomial and multinomial PDFs, and weighted sums to model trust.

As showcased in Table 4, Bayesian Theory proved its practicality in several cases. Zhang et al. [50] proposed An Anti-Attack Trust Management Scheme (AATMS). AATMS is meant to be resistant against newcomer (e.g., or WW), OO and CL attacks. AATMS considers Bayesian inference to compute direct trust relationships based on local and past interactions, adopting in parallel a variation of PageRank [79] for global trust computation. The trust model proposed by Chen et al. [51] builds direct trust using a Bayesian inference model based on the beta PDF. In the approach from [51], the generated trust values are used in a k-means [80] based recommendation filtering approach to determine outlier nodes (e.g., untrusted nodes).

Another notable work is that of Rajeswari et al. [52], which introduced two distinct trust-based algorithms. The first algorithm is an energy-efficient clustering approach. As for the second algorithm, an untrustworthy filtering recommendation algorithm was considered. In both approaches, direct trust is computed using beta PDF. The output trust values are further used to build the filtering algorithm meant to mitigate trust attacks.

Targeting specifically cognitive radio networks, a notable mention is the work of Fu and He [53], who proposed a Bayesian inference trust model with sliding window to identify spectrum sensing data falsification attacks. Similarly, Gao et al. [54] considered a sliding window approach to compute trust values to keep the influence of historical interactions. Additionally, Gao et al. [54] introduces a penalty factor to put more significance on more recent interactions.

Saidi [55] introduced a trust model that focuses on determining behaviour similarity between network nodes through Jaccard distances. First a bipartite graph representation of the network is computed, and based on the edge similarity, which ultimately expresses the trust relationship, the similarity coefficient is computed to eliminate malicious nodes. Tackling the problem of intrusion detection there are also the works of Teng et al. [56] and Abhishek and Lim [57]. Teng et al. [56] considered a Bayesian trust model for direct trust, with a fuzzy-based indirect trust approach. Additionally, the authors introduced a comprehensive trust attribute denoting a weighted sum obtained from direct and indirect trust. A trust path evaluation methodology was considered to detect BH attacks. On the other hand, Abhishek and Lim [57] proposed a sufficient statistical-based model for trust computation, with an aggregation approach established on weighted sums to fuse trust values. Additionally, a Gaussian kernel-based similarity metric [81] was considered to differentiate malicious nodes from benign ones.

Ren and Qin [58] proposed a trust fusion scheme that combines the Jensen-Shannon divergence measure [82] with an analytic hierarchy process to fuse decision factors. The authors' trust evaluation and fusion approach shows promising results in terms of efficiency, scalability and resilience from the theoretical analysis conducted.

Qureshi et al. [59] presented a Cumulative Trust Evaluation based Efficient Technique (CTBET). CTBET fuses direct and indirect trust values (i.e., computed using QoS statistics) to protect IoT devices against OO or BM trust attacks. Resistance against attacks also represented a focal point for Jabeen et al. [60]. To combat trust attacks such as BM or SB, a QoS based approach was undertaken to build their trust model. Kalkan and Rasmussen [61] developed another relevant framework titled Trust Framework for Service Discovery (TruSD), in which trust-based service discovery happens through a distributed hash table. Moreover, there is also the work from Wang et al. [67], where a multilayered TMM framework was introduced targeting trust at fog level in IoT systems.

Focused on the fog level, there is likewise Zhang et al. [62]. The authors explored the possibility to detect at fog level hidden data manipulation attacks. Several trust metrics were examined (e.g., QoS and routing metrics) for outlier detection. Similarly, the authors of [63] developed a fog-based distributed trust and reputation system based on summed weighted trust metrics. Other similar approaches based on statistical measurements and weighted sums are [64], [65], and [66].

Bayesian and statistical models are equipped with the necessary formalism to address both, direct and indirect trust computation. Moreover, works like [59] and [79] go a step further and combine the two trust values under a common

TABLE 4. Overview of bayesian theory and statistical models. (✓- considered, ✗- not considered, ∼ - partial considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[51]	VANET	Bayesian inference based model empowered by a TrustRank variation method to compute global trust values.	WW, OO	✓	✓	✓
[52]	IoT	Trust computed using the beta reputation system, together with a recommendation filter for malicious advertisements.	OO, SYB, BM, SB	✓	✓	✓
[53]	MANET	Trust estimation using beta distribution, together with a clustering algorithm to filter untrustworthy recommendation.	GEN	✓	✓	∼
[54]	IoT	Bayesian inference based model with sliding window.	MITM	✓	✓	✓
[55]	VANET	Bayesian inference based model over historical data, together with a penalty factor and time decay function to model trust.	N/A	✓	✓	✗
[56]	WSN	Untrusted node detection using Jaccard distance.	SB, BH, MITM	✗	✗	✓
[57]	WSN	Bayesian trust model for direct trust with a fuzzy-based approach for indirect trust modelling to mitigate BH attacks.	BH	✓	✓	✓
[58]	VANET	Trust-based intrusion detection system for identifying malicious vehicles.	GEN	✓	✓	✗
[59]	IoT	Trust fusion using Jensen-Shannon divergence measure with decision fusion based on a analytical hierarchical process.	SB, OO	✓	✓	✓
[60]	IoT	Trust-based approach to detect and isolate malicious misbehaving nodes.	OO, BM	✓	✓	✓
[61]	IoT	Probability and weighted sum based TMM.	CL, BM, SB	✓	✓	✓
[62]	IoT	Developed a trust-based framework for service discovery using distributed hash tables.	OO, BM, SB	✗	✓	✓
[63]	WANET	Hierarchical trust evaluation based on network Quality of Service (QoS) evidences.	CL	✗	✗	∼
[64]	IoT	Distributed trust and reputation system.	BM, OO, SB	∼	✓	∼
[65]	IoT	Centralised sum-based trust model for IoT resource sharing.	OO, BM, WW	✓	✓	✓
[66]	VANET	Distributed trust-based coalition formation for autonomous vehicles using game theory.	MITM, SYB, CL	✗	✓	✓
[67]	IoT	Trust-based evolutionary game model for managing IoT federations.	BM	✓	✓	✓
[68]	IoT	A Multilayered TMM framework at fog level. Trust modelled based on weighted sums.	GEN	✓	✓	✓
[69]	WSN	Probabilistic graph trust model aimed to monitor the network trust state.	GEN	✗	✓	∼
[70]	WSN	Hidden Markov Model for dynamic sensor behaviour modelling.	N/A	✗	∼	✗
[71]	Edge	Multi-source trust fusion algorithm.	N/A	∼	✓	✗
[72]	VANET	Edge-centric probability-based TMM for deploying trusted agents.	BM, SYB	✓	✓	✓
[73]	IoT	Trust-aware greedy algorithm for selecting high trusted nodes.	N/A	✓	✓	✗
[74]	IoT	Context-based trust evaluation system with dynamic weight factors.	BM	✓	✓	✓
[75]	IoT	TMM for secure device to device communication in 5G networks.	OO, SB	✓	✓	✓
[76]	IoT	Trust inference model using the beta. Probability Density Function (PDF).	N/A	✓	✓	✗
[77]	IoT	Weighted sum and Naive Bayes classifier to compute reputations.	N/A	✗	✓	✗
[78]	VANET	Forest Fire based model for minimum number of broadcaster nodes for emergency message dissemination.	N/A	✗	✓	✗

global attribute, expressing a general or collective trust perspective. Computational models such as [54] demonstrate how traditional theory can be expanded with trust related functionalities (e.g., penalty factors). Likewise, we observed that the models analysed in this section, do not only approach trust from a Bayesian or statistical point of view, but rather merge this theory with other related methods (e.g., clustering [52], fuzzy theory [56]), similarity metrics (e.g., Jensen-Shannon divergence [58], Jaccard distance [55]) or data processing techniques [53], [54].

B. CLUSTERING MODELS

Clustering solutions aid DWNs by providing a node grouping mechanism on-top of the ad-hoc, dynamic infrastructure [83]. In general, a clustering approach entails as a first step a Cluster Head (CH) election procedure. The main responsibility of a CH is to act as a cluster's or group's leader, coordinating the communication in the current cluster and forward necessary packets to neighbouring clusters. By having multiple small clusters instead of a single one, several networking improvements are achieved. The number of links that must be maintained by each cluster member is reduced, energy consumption consecutively is improved, therefore the network becomes more scalable, obtaining the ability to dynamically update clusters as the number of nodes increases or decreases.

Clustering has been a popular approach among researchers for many years, resulting in a wide range of clustering methodologies being developed [101]. Clusters are formed based on a set of criteria and procedures. Some popular choices include connectivity models or hierarchical clustering [102], centroid models such as k-means [103], density-based models [104], c-means or fuzzy c-means [105], to mention a few. While the algorithms target clustering analysis, they also paved the road for ad-hoc clustering solutions. Ad-hoc network clustering received in the same manner considerable attention, forming a consistent ground of techniques addressing clustering problems. One of the most well-known works in the field is Low Energy Adaptive Clustering Hierarchy (LEACH) developed by [106], where a hierarchical clustering algorithm is offered aiming to reduce the energy consumption of nodes. A similar solution, focused on minimising energy consumption is that of [107] where Hierarchical Energy-Efficient Distributed clustering (HEED) was proposed. Other known methods are Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [108] or Adaptive Power-aware ID-based Trust clustering (APIT) [109]. A summary of trust clustering-based approaches is depicted in Table 5.

A Stable and Centralized Trust-Based Clustering (Stab-Trust) was proposed by Awan et al. [84] targeting VANETs. In this work, the authors leverage a trust-based CH election mechanism with the capability of isolating malicious nodes from the cluster formation protocol. Another CH selection mechanism was additionally offered by Saidi et al. [85]. A notable contribution of Saidi et al. [85] is the ability of their method to isolate compromised or malicious CHs, while preserving at the same time the network performance. On the same topic, Amuthan and Arulmurugan [86] investigated the possibility of applying a Semi-Markov scheme to improve the network lifetime in the process of CH election. Lastly, Veeraiah et al. [87] suggested fuzzy clustering as a promising approach to select CH to aid in multi-hop routing, while maintaining an optimal energy consumption.

In the direction of identifying misbehaving nodes, the work of Montenegro et al. [88] successfully applied k-means clustering for detecting anomalous un-trusted nodes. Following the same method, Ma et al. [89] proposed a distributed consensus trust model to evaluate nodes trustworthiness. In their work, node misbehaving is detected via k-means clustering. Targeting packet manipulation attacks, Liu et al. [90] tackled a regression-based approach together with a clustering algorithm to classify nodes as benign or malicious. Yang et al. [91] investigated the problem of outlier detection in WSNs with a fuzzy-based trust evaluation methodology, to achieve a balance between energy consumption and security in the CH election process. Distinct from the aforementioned works, Padmaa et al. [92] considered a model involving oppositional chaos game optimisation clustering for cluster construction and leader election. Lastly, Pedroso and Santos [93] tackled the problem of false data injection attacks by designing a consensus-based data filtering approach, where a clustering and a fault module are entailed to solve the problem.

The data privacy and anonymity dimension involved in the clustering process was addressed by Guo et al. [94]. In their work, the authors focus on overcoming privacy issues by adopting a K-anonymity [124] method to create anonymous groups. Trust values are considered in group formation to enforce an incentive-based cooperation mechanism between nodes. Likewise, Farman et al. [95] proposed a privacy oriented CH election algorithm. The selected CH serves as a *phantom* node, aiding the network to load balance better the network traffic.

C. ROUTING TRUST MODELS

The decentralised nature and the fact that ad-hoc wireless networks do not rely on a pre-existing infrastructure, motivated a handful of researchers to investigate the problem of efficient routing in this environment. While clustering algorithms intend to provide a mechanism for node coordination and network structure formation at application level, efficient message routing represents the next step in network organisation. The maturity of the field is shown by the numerous papers published on this topic and the proposed extensions of well-known protocols. Perkins et al. [125] designed Ad-hoc On-demand Distance Vector (AODV) by leveraging distance vectors for mobile ad-hoc network routing, while Johnson et al. [126] built Dynamic Source Routing (DSR) following a source routing approach, where the source node is responsible to decide where to forward the next packet. Priory, Perkins and Bhagwat [127] introduced Destination-Sequenced Distance-Vector Routing (DSDV), a protocol based on the Bellman-Ford algorithm [128] and distance vectors, which targets low mobility networks. Likewise, the Temporally-Ordered Routing Algorithm (TORA) protocol was proposed by Park and Corson [129], as a solution based on the link-reversal algorithm for highly mobile ad-hoc nodes.

Naturally, each protocol has its own advantages and disadvantages, depending on a set of specific requirements. Routing protocols in ad-hoc wireless networks evolved over time, multiple variations of known protocols and newer implementations appeared in the past years, having TMM as a focal point. The additional novelty brought by TMM in routing protocols is the aspect of allowing nodes to create and maintain their own group of trustworthy neighbours with which they can cooperate to safely move packets across the network. Conversely, un-cooperative and malicious nodes represent the main threat to the network well-being. Table 6 offers additional information on the works presented below.

TABLE 5. Overview of trust-based clustering approaches. (✓- considered, ✗- not considered, ∼ - partially considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[85]	VANET	Centralised trust-based CH selection approach.	SYB, BH	✓	✓	✓
[86]	WSN	Trust oriented CH election algorithm capable of isolating misbehaving nodes.	SB, BH	✓	✓	✓
[87]	WSN	Semi-Markov CH election scheme using an energy-trust assessment.	N/A	✓	✓	✗
[88]	MANET	Fuzzy clustering approach based on trust values.	GEN	✓	✓	✗
[89]	VANET	K-nearest neighbour for direct trust computation based on distances between vehicles.	GEN	✗	✗	✗
[90]	IoT	K-means clustering anomaly detection for un-trusted nodes.	SB, BH, BM	✓	✓	✓
[91]	IoT	Analysed the performance of multiple clustering approaches combined with regression methods to detect conditional manipulations of packets.	SB	✓	✓	✓
[92]	WSN	Fuzzy clustering with a density-based outlier detection solution.	MITM, SB	✓	✓	✓
[93]	IoT	CH selection with secure route identification. Trust verification using fitness function.	N/A	✓	✓	✗
[94]	IoT	Consensus based data filtering to mitigate false data injection.	IMP	✓	✓	✓
[95]	IoT	A trust and privacy technique based on K-anonymity and beta PDF.	N/A	✓	✓	✗
[96]	VANET	Privacy preserving trust model to elect CHs. Stability parameter checking with Sensitivity analysis.	N/A	✗	∼	✗
[97]	IoT	Cluster formation approach based on trust metrics and interactions between nodes.	BM	✓	✓	✓
[98]	VANET	Incentive-based game theory approach to filter malicious vehicles.	BH, OO, SYB	✗	✓	✓
[99]	IoT	Developed a distributed framework with a reputation-based clustering approach.	N/A	✗	✓	∼
[100]	WSN	Multidimensional two-tier hierarchical trust evaluation for CH selection.	N/A	✓	✓	✗
[101]	IoT	Proposed a broker-based variation of k-means with trust weights designed to enhance reliability of IoT services.	BM, SB, CL	✓	✓	✓

TABLE 6. Overview of trust-based routing approaches. (✓- considered, ✗- not considered, ∼ - partially considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[111]	MANET	Trust model for secure routing based on several trust attributes.	BH, BM, CL	✓	✓	✓
[112]	MANET	Routing algorithm based on trust entropy, assisted by a Petri net cloud trust model.	BH	✓	✓	✗
[113]	IoT	Efficient energy aware trust model for improved routing.	BH, SYB, OO	✓	✓	✓
[114]	WSN	Multi-hop trust evaluation approach for secure routing.	N/A	✗	✓	✗
[115]	WSN	Weighted clustering for node grouping and optimal routing using oppositional based learning.	N/A	✓	✓	✗
[116]	WSN	Link failure detection for dynamic selection of shortest path.	GEN	✓	✓	∼
[117]	WSN	Secure multi-factor routing protocol in clusters of sensors.	BM, WW, OO	✓	✓	✓
[118]	WSN	Trust-based adaptive genetic algorithm for energy efficient routing.	BH, SB, BM, OO	✓	✓	✓
[119]	WSN	Extended the LEACH routing protocol with trust metrics to improve energy consumption.	SB	✓	✓	✓
[120]	WSN	Opportunistic routing algorithm based on direct and indirect trust values.	SB	✗	✓	∼
[121]	WANET	Sensor clustering formation algorithm with trusted secure routing.	GEN	✓	✓	✓
[122]	MANET	Resource consumption Reputation-based model,	MITM, SB	∼	∼	∼
[123]	IoT	Bayesian model with Fuzzy-based decision making for routing.	MITM, BH	✓	✓	✓
[124]	VANET	Hybrid trust model for secure routing aimed at avoiding network disconnections.	N/A	✓	✓	✗

One of the first works found in the time frame considered in the present survey targeting trust-based routing, is that of Qu et al. [110] where the authors analysed the possibility of implementing a secure trust model-based routing approach for mobile Peer-to-peer (P2P) networks, with the possibility of identifying non-cooperative nodes using a cosine similarity method [130], [131]. Wang et al. [111] proposed a cloud-assisted trust model to empower secure routing, where the trust reasoning model leverages Petri nets to evaluate the credibility of nodes. Additionally, the concept of trust entropy is introduced as a decision making process to select routes with least entropy for optimal packet transmission.

A notable work is that of Khan et al. [112]. Here, a Trust-based Efficient Routing Scheme (ETERS) was proposed, together with CH selection strategy. Thorough experimentation demonstrated the efficiency of ETERS against a wide range of trust attacks. Additionally, their beta distribution approach in ETERS is demonstrated to be sounder than Gaussian or Dirichlet variations.

The problem of multi-hop routing was the focus for two distinct works. Desai and Nene [113] introduced a normative and an empirical trust evaluation routing approach. The authors presented the concept of trust circles, used to evaluate trust values over multiple hops. In parallel, Hilal et al. [114] addressed further the problem of multi-hop routing by designing Trust Aware Oppositional Sine Cosine-based Multihop Routing (TAOSC-MHR). TAOSC-MHR is built over a weighted clustering scheme to divide and create trusted node clusters. After a CH is selected, TAOSC-MHR selects the optimal multi-hop route with the help of an Oppositional Based Learning method, and a Sine Cosine Optimization algorithm [132]. In the same manner, link failure detection is a critical aspect in multi-hop routing. Srividya et al. [115] addressed this problem by introducing a weighted trust-based end-to-end mechanism for link failure detection.

Energy consumption is a crucial consideration when developing methods for sensor networks. Consequently, this problem if often treated in ad-hoc routing. For example, Khan et al. [116] developed ETERS. Like TAOSC-MHR, ETERS entails first a CH selection process. Furthermore, ETERS models trust based on the beta PDF, and additionally incorporates an attenuation factor during trust evaluation to better reflect the impact on trust of external factors. In [117], the authors proposed Trust-Based Adaptive Genetic Algorithm (TAGA) as an approach resilient to not only known routing attacks, but also to trust attacks. While one of the scopes of TAGA is to minimise energy consumption caused by data transmission, TAGA further introduces a threshold function for CH selection, an adaptive penalty factor in trust computation, and a genetic algorithm to optimally find the safest paths for the CH to route packets. Other works cover energy related problems, such as [118], where the authors conducted an analysis of energy attacks for the LEACH protocol [106], and proposed an energy drainage detection mechanism along a trust-based protocol for CH selection and routing. Along with energy, resource consumption poses an additional significant criteria while working with sensors. This constraint was prioritised by Zhao and Srivastava [119], where an opportunistic trust-based routing algorithm was proposed. The intrusion detection aspect on routing protocols was approached by two works. While the authors of [120] addressed this topic by a false data injection detection mechanism, Fayaz et al. [121] focused on identifying selfish nodes intending to compromise the reputation of benign nodes.

Sadayan and Ramaiah [122] combined the properties of fuzzy logic in parallel with a Bayesian statistical model to efficiently route packets in high mobility MANETs. While fuzzy logic is employed to compute trust values, the Bayesian model was consider to predict the next hop. Routing in mobile networks was additionally explored by Bhende et al. [123]. The authors targeted VANETs, developing a method capable of discovering unreliable (e.g., untrustworthy) vehicles in packet routing.

D. BELIEF THEORY MODELS

The social aspect, together with the fact that trust is deeply tangled with reasoning under uncertainty, made Belief Theory (BT) a popular choice for researchers interested in modelling trust in cooperative wireless networks. Also known as Dempster-Shafer Theory (DST) of evidence [133], the approach provides a robust framework helpful in representing uncertainty and incomplete information, or in fusing multiple sources of evidence under a single value. Rooted in Bayesian theory, the main building block of the DST is the concept of belief function, which ultimately is meant to assign a degree of belief to a set of propositions. The degree of belief is expressed as a numerical value in the range of 0 to 1, where 0 can expresses total disbelief, and 1 – total certainty. Following this rationale, there is a parallel between uncertainty or belief and trust.

In the domain of VANET, DST was considered as an appropriate trust aggregation technique to compute global trust scores by Sayed et al. [134]. Direct trust values are computed based on the vehicle's behaviour and are fused together with propagated indirect trust values under a single value. This final global trust value is utilised as a mechanism to punish or reward benevolent and misbehaving vehicles. In the same context and direction, the work of Bhargava and Verma [135] leverages DST. Furthermore, the authors introduced several functions to empower DST, such as a penalty, forgetting, rewarding and uncertainty-based functions. Lastly, the authors proposed an additional weight in the process of trust update, denoted as a forgiving factor, that is meant to stimulate positive behaviour when an untrusted node starts to behave normally. Targeting Connected Autonomous Vehicles (CAVs), Halla-aho et al. [136] offered a short work with conceptual design for trust parameters of CAVs with evaluation using DST.

The area of IoT and WSNs was likewise covered by three distinct works. Misra et al. [137] proposed Secure Range-based Localization with Evidence Theory (SecRET), specifically targeting underwater sensors. SecRET enables unlocalised sensors to find the most reliable nearby nodes by leveraging a series of trust-based computations. To efficiently compute trust values, trust metrics such as packets forwarded, residual energy, indirect trust recommendations, and the

TABLE 7. Overview of BT models. (✓ - considered, ✗- not considered, ∼ - partially considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[135]	VANET	Hierarchical trust management, combining Bayes theorem for local trust, DST for trust aggregation, and a platoon-based dissemination propagation model.	OO, BM, SB	✓	✓	✓
[136]	VANET	Introduced several trust related factors to better categorise trust in networks of vehicles using DST.	N/A	✓	✓	✗
[137]	VANET	Conceptual design of a trust parameters evaluation tool using DST.	N/A	✗	✗	✗
[138]	WSN	DST based trust model for autonomous identification of trustworthy underwater anchor nodes.	SB, BM, OO, MITM	✓	✓	✓
[139]	IoT	Decentralized trust model based on DST for trust score aggregation.	GEN	✗	∼	✗
[140]	IoT	Trust model based on Transferable Belief Mode for mobile agents.	N/A	✓	✓	✗

consistency of data transmitted by neighbouring sensors are considered. Ultimately, SecRET is an effective approach strong against malicious nodes, capable of detecting faults in uncooperative sensors.

Esposito et al. [138] combined the fusion properties of DST over trust values with a game theory approach and a decentralised ledger for trust management. Finally, Rajavel et al. [139] developed Trust-Aware Pricing Scheme for Edge-Based Mobile Sensor-Cloud (MobiTrust). It considers a game theoretical pricing scheme to ensure trust in the edge based on the Stackelberg game [140]. Furthermore, MobiTrust provides a mobility-aware trust model based on a Transferable Belief Model, which ultimately is an extension of the DST.

Additional information about the works described above is outlined in Table 7.

E. SUBJECTIVE LOGIC MODELS

Similarly to BT, SL offers a framework helpful when reasoning under uncertainty is a necessity. SL combines concepts brought from probabilities and logic, together with aspects including uncertainty and subjectivity in decision making [47]. SL defines a belief under the form of an opinion metric, which manifests uncertainty and degrees of ignorance about a subject (e.g., trust) [148]. An opinion in SL can be expressed under many forms [47], but in general, it is a function composed of four distinct states: belief, disbelief, uncertainty, and a base rate. Furthermore, opinions can be mapped to a beta PDF over binary events, where the PDF's arguments express the number of positive and negative past observations.

SL defines a set of operators which can be applied to work with opinions. The most frequently used operators are the transitivity and fusion or consensus. By computing a transitivity operation between two opinions, an agent A (e.g., sensor) forms an opinion about C, using B's opinion of C. This is also known in the literature as a referral or recommendation of opinion or trust. The fusion or consensus operator has the purpose to merge two or more opinions, possibly conflicting, under a single opinion to achieve consensus.

These core features offered by SL are frequently leveraged in the literature of TMM to solve trust related problems in fields such as IoT or Social Internet of Things (SIoT). Alemneh et al. [141] proposed SL as a basis for a two-way TMM technique. The authors created the opportunity for IoT nodes to evaluate the trustworthiness of service providers in the IoT fog layer. To accomplish this, Alemneh et al. [141] opted to use QoS related trust metrics (e.g., latency, packet delivery ratio) and social-based ones (e.g., ownership, honesty). Similarly, Wei et al. [142] proposed a bidirectional trust model to address trust issues regarding service delegation in IoT. Consequently, SL was considered adequate to help isolate malicious service providers running at fog level from benign ones.

The problem of identifying and isolating malicious agents was likewise addressed by taking advantage of the properties of SL. Al Muhtadi et al. [143] proposed an initialisation method for SL to address the problem of *cold-start*. Their approach sets initial opinion values for trusted nodes with a belief set to 1, disbelief and uncertainty to 0. These initial values, together with a base rate of 1, eliminate the uncertainty aspect, which would create dogmatic opinions for trusted nodes in the end. Oliveira et al. [144] proposed ELECTRON, a trust-based access control solution developed over SL, capable of establishing trust groups using the interaction between the nodes of an IoT network. Wang et al. [145] tackled the subject of computing trust chains based on the interactions between nodes in IoT, assessing in parallel possible risks and threats that come up in IoT scenarios. Regarding IoT threats, Prathapchandran and Janani [146] opted to develop a solution tailored for sinkhole attacks (i.e., BH attack) where a Random Forest approach together with a SL model is considered.

Additional information about the works described above is summarised in Table 8.

F. FUZZY THEORY MODELS

Fuzzy theory represents the theoretical groundwork for fuzzy logic [156]. While fuzzy logic deals with reasoning where a fixed answer is not required, but only an approximation of it, fuzzy theory on the other hand branches out into computer science providing mechanisms for reasoning and

TABLE 8. Overview of SL models. (✓- considered, ✗- not considered, ∼ - partially considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[142]	IoT	Two-way TMM based on SL.	SYB, BM, OO	✓	✓	✓
[143]	SIoT	Bidirectional model based on SL.	N/A	✗	✓	✗
[144]	IoT	Application of SL at node level in IoT.	N/A	✗	✗	✗
[145]	IoT	Social trust access control based system using SL.	SYB	✓	✓	∼
[146]	IoT	Trust chains computation using SL. Extended Dijkstra algorithm with trust information.	SB	✓	✓	✓
[147]	IoT	SL and random forest trust model.	BH	✓	✓	✓
[148]	WSN	Extended the beta reputation system with a threat coefficient to emphasise negative behaviours.	GEN	✓	✓	✓

TABLE 9. Overview of fuzzy theory models. (✓- considered, ✗- not considered, ∼ - partially considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[150]	IoT	A fuzzy analysis for identifying and prioritising trust metrics.	N/A	✗	✓	✗
[151]	IoT	Fuzzy-based trust evaluation of fog nodes based.	N/A	✗	✓	✗
[152]	VANET	Fuzzy c-means, K-nearest neighbour (KNN) based trust model to deal with un-trusted sources of information in VANET.	MITM, BM, OO	✓	✓	✓
[153]	WSN	Fuzzy-based group formation based on trust metrics.	GEN	✓	✓	✓
[154]	MANET	Fuzzy-based mechanism for identifying groups of non-legitimate nodes in smart city networks.	CL.	✓	✓	✓
[155]	WSN	Fuzzy-based trust model with an artificial bee colony algorithm for malicious node identification.	BM, CL	✗	✓	✓
[156]	IoT	Fuzzy-based trust model tailored to detect SYB attacks.	SYB	✓	✓	✓

decision-making under uncertainty. Ultimately, fuzzy theory offers a robust mathematical framework capable of working with incomplete information by employing fuzzy sets and logic. The concept of fuzzy sets encapsulates a group of membership functions that map a set of input values to a degree of membership in the fuzzy set. Consequently, the degree of membership is a value in the range of 0 to 1, where the first represents no membership, and the latter full membership. The concepts behind fuzzy theory became helpful when the system model cannot be described by Boolean logic. As such, fuzzy theory grew into a potential candidate in solving problems in numerous research fields, such as natural language processing, industrial control systems, artificial intelligence and decision making systems.

While providing a framework similar to the one offered by DST, fuzzy theory found its application in the context of TMM in a handful of papers and problems. An interesting work was proposed by Ogundoyin and Kamil [149], in which a fuzzy analytic hierarchical process technique was considered appropriate to investigate the possibility of identifying and prioritising trust parameters. Their study indicated that the most prioritised parameter is QoS, while the least prioritised is the trust recommendation.

Rahman et al. [150] considered a broker-based framework for trust evaluation at network fog level. The scope of the work is focused on determining the most trustworthy fog node to fulfil user requests. Fuzzy logic is explored as basis to evaluate trust in nodes by taking in consideration trust metrics such as node availability, QoS, security, user feedback, and cost. Plausibility, experience and node's type are several trust metrics considered by Soleymani et al. [151] in their fuzzy trust model. Tailored for VANETs, the author's model deals with untrusted sources of events coming from the vicinity of vehicles. The authors tested their model under line of sight and none-line of sight VANET conditions. Other trust metrics, for instance, distance, energy and relative mobility were considered by Krishnaswamy and Manvi [152] in their fuzzy model. The scheme in [152] is accompanied additionally by a simple XOR-based authentication scheme as a preliminary step before determining node's trust.

Secure approach for Smart city Environment by Accusation based List (Secure SEAL) was introduced by Simpson and Nagarajan [153] as a promising solution to deal with groups of malicious untrusted nodes colluding to compromise a large scale IoT trusted network. The authors focused on fuzzy theory to establish the trustworthy environment and to ensure fast detection of colluding groups. Once tagged as untrusted, nodes are isolated from the network, and at a later time, a re-evaluation takes place to reconsider the node trust. While the re-evaluation was considered as a mechanism to limit accidental exclusion of normal nodes, a question is raised on how the model proposed by [153] behaves in front of OO attacks, where a malicious node intentionally switches between benign and malicious behaviour. Likewise, Almogren et al. [155] focused their model on preventing one specific TMM attack: SYB. In this attack a malicious actor steals or claims the identity of a legitimate node for self and biased advertising. Their fuzzy model evaluates trust by considering node neighbourhood's integrity, receptivity and compatibility.

Additional information about the works described above is recapitulated in Table 9.

G. MACHINE LEARNING MODELS

Machine Learning (ML) models are excellent in solving TMM problems due to several properties they possess. In general, TMM techniques intend to model the behaviour of a set of network members to determine deviations from a baseline, which in the end may be considered untrusted behaviour. Similarly, ML models proved to be capable of handling this task with ease with outlier/anomaly detection or classification approaches [177]. A parallel can be made between ML anomaly detection and determining the trust level of a node in a network. Ultimately, untrusted nodes represent the outliers or anomalies, while the trusted node behaviour represents the baseline that must be learned by the ML model. Consequently, this further implies data availability for model training, in comparison to other TMM models that do not require this step (e.g., Bayesian models, DST models). Besides outlier detection, behaviour modelling and classification, ML models are considered in TMM trust fusion, offering a potential solution of aggregating multiple sources of data points under a common denominator. The variety of ML models applied, and their targeted problem can be observed in Table 10.

Huber and Kandah [157] offered a comparison of various ML classification models (e.g., Decision Trees, KNN, Support Vector Machine (SVM), Multi-layer Perceptron (MLP)) to evaluate their efficiency in establishing a trusted baseline behaviour of VANETs, to detect outlier (e.g., untrusted) behaviour. Similar models were also considered by Hei et al. [158]. In their work, the authors considered a decentralised learning approach, where federated learning is combined with a decentralised ledger in the IoT environment. While the ledger is used as a permissioned blockchain to store and distribute detection alerts of attacks, several ML models were analysed (e.g., MLP, Decision Trees, Random Forest, SVM) in the context of federated learning. Wang et al. [159] likewise investigated the possibility of applying federated learning in the context of heterogeneous VANET trust environments. Behavioural modelling was also considered by Ma et al. [160], which entailed a Long Short-Term Memory (LSTM) NN to build a baseline model trained on QoS trust properties to detect similarities between the real and modelled IoT devices.

Juneja et al. [161] focused on detecting energy related trust attacks aiming to deplete nodes' battery. Additionally, the proposed approach intends to aid secure routing in WSNs by avoiding malicious nodes. Another work using this model proposed a Deep Q-Network algorithm with a deep reinforcement learning model for task offloading trust evaluation Tong et al. [162]. On a similar note, He et al. [163] suggested a trust update mechanism based on reinforcement learning targeting underwater acoustic sensor networks. Lastly, the work of Lin et al. [164] considers reinforcement learning as a data fusion approach. Their model is empowered with a transfer learning algorithm to reduce training time and a dynamic punish-reward mechanism to manage node behaviour is provided.

On the topic of intrusion detection, the work of Bhor and Kalla [165] employed a Taylor-spider monkey optimisation-based belief NN trained on trust values. Similarly, with a focus on detecting trust attacks, Magdich et al. [166] considered a classification approach with feed-forward NNs. Awan et al. [167] additionally addressed this challenge by proposing a recurrent NN to predict malicious behaviour of nodes in IoT. The approach showed relevant results in detecting numerous trust attacks (e.g., BM, WW, SB). Abdalzaher et al. [168] focused on attack detection, not specific to TMM, and investigated the problem of detecting jamming attacks in the context of IoT through an auto-encoder-based approach.

Alqahtani et al. [169] proposed a modified trust-based feed-forward NN to monitor IoT networks and protect them against unauthorised access. El-Sayed et al. [170] considered Feed-forward NN along a Decision Tree approach to evaluate trust in the VANET ecosystem.

Zineddine [171] proposed a fuzzy-based NN combined with a weighted weakest link algorithm to classify fog nodes based on their trust values. The work showed promising results with a model accuracy of 0.9996. A similar approach was undertaken by [172] which considered a fuzzy neural network for data fusion in IoT.

H. SOCIAL-BASED MODELS

Social inspired trust models aim to integrate trust concepts (e.g., trust metrics) from disciplines such as Sociology, Psychology or Economics in the domain of Information Technology. In comparison to the models mentioned in previous sections, which focus more on handling uncertainty or dependability between past interactions, social-based models intend to additionally model social trust factors raging from confidence and experience to frequency and honesty [6]. In other words, social-based models incline to bring the characteristics of human-to-human interactions in the digital space. So far, the works identified on this topic in our survey assume the presence of the human factor in the system, while others are inspired by social phenomena in model design. As an outcome, research fields like SIoT bring the social aspect of human trust in conjunction with that of device-to-device interaction in a hybrid environment. As seen in Table 11 a handful of works investigated social-based trust models.

TABLE 10. Overview of machine learning models. (✓ - considered, ✗- not considered, ∼ - partially considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[158]	IoT	Vehicle behaviour modelling using anomaly detection to detect behaviour deviations.	SB, CL, SYB	✗	✓	✓
[159]	IoT	Intrusion detection based on federated learning approach.	GEN	✓	✓	∼
[160]	VANET	Hierarchical trust evaluation model for node ranking based on federated learning.	GEN	✓	✓	∼
[161]	IoT	Trust-based long-short term Neural Network (NN) with sliding window to aggregate QoS trust properties and build a behavioural model for IoT devices.	GEN	✓	✓	✗
[162]	IoT	Reinforcement learning using a policy gradient algorithm.	N/A	✗	✓	✗
[163]	IoT	Deep Q-Network algorithm with a deep reinforcement learning model for task offloading trust evaluation.	N/A	✓	✓	✗
[164]	WSN	Trust-based node sensitivity estimation. Trust update with reinforcement learning.	MITM, SB	✓	✓	✓
[165]	IoT	Deep reinforcement learning trust evaluation models, with a reward and punishment system to encourage collaboration.	GEN	✗	✓	✓
[166]	IoT	Intrusion detection based on Taylor-spider monkey optimisation belief network using trust metrics extracted from KDD dataset.	GEN	✓	✓	∼
[167]	SIoT	Threat detection based on trust rating score for communication safety.	SB, BM	✓	✓	✓
[168]	IoT	Recurrent NN trained on trust metrics to detect malicious node behaviour.	BM, WW	✓	✓	✓
[169]	IoT	Detection of jamming attacks using deep autoencoders.	N/A	✗	✓	✗
[170]	IoT	Trust-based monitoring system against unauthorised network access.	SYB	✓	✓	✓
[171]	VANET	Average and Euclidean distance-based trust model, with a neural network to ensure reliable message transmission.	GEN	✗	✓	∼
[172]	IoT	Classification of fog nodes based on trust values, using fuzzy machine learning and weighted weakest link.	N/A	✓	✓	✗
[173]	IoT	Trust-based fuzzy NN for data fusion in IoT.	N/A	✓	✓	✗
[174]	IoT	Support vector machine model to detect trust related attacks.	SB, OO, WW, BM, SYB	✓	✓	✓
[175]	IoT	Trust threshold estimations using a support vector machine approach.	SB	∼	∼	∼
[176]	WANET	Neural network for estimating trust values for routing, following a protocol agnostic approach.	N/A	✗	✓	✗
[177]	IoT	Variational auto-encoder for trust modelling.	N/A	✗	✗	✗

TABLE 11. Overview of social-based models (✓ - considered, ✗- not considered, ∼ - partially considered).

Source	Domain	Description	Resistant against	C1	C2	C3
[179]	VANET	Message dissemination between vehicles using social relationships.	N/A	✓	✓	✗
[180]	SIoT	Weighted-kNN to aggregate trust ratings and detect discriminating behaviours.	BM, SB	✓	✓	✓
[181]	P2P	Files and peers trust classification based on the concept of Hadith.	CL, MITM, SB	✓	✓	✓
[182]	SIoT	Friend choosing algorithm based on social ties developed between nodes.	N/A	✓	✓	✗
[183]	SIoT	Hybrid TMM based on human-device interaction.	BM, SYB, SB, OO	✗	✓	✓
[184]	SIoT	Context-depended trust management for SIoT job allocation.	WW, BM, SB, OO, CL	✓	✓	✓

The problem of message dissemination in the context of social VANETs was investigated by Ullah et al. [178]. Here, a trust and reputation mechanism to determine false advertisements between vehicles was employed. To achieve this, social ties were constructed and maintained between vehicles by taking into consideration the vehicle behaviour, the vehicle-to-vehicle interactions, and the vehicle contributions to the network.

An interesting work was also brought up by Jafarian et al. [179] that introduced Discriminative-aware Trust Management (DATM), utilising a weighted-KNN to aggregate ratings in a given time period on certain service providers in SIoT. It considers trust metrics such as social similarity, importance of the service, and energy in trust modelling. Ultimately, DATM isolates malicious IoT objects to prevent discriminatory behaviour against trusted objects. On a similar note, Alqahtani et al. [180] proposed HadithTrust, where network peers and files are systematically classified into multiple levels of trusts. Trust is determined with set of narrators (e.g., trusted peers) advertising about a specific neighbour or file. Peer behaviour or file content is examined to determine trust levels together with information dispersed by recommander nodes (i.e., narrators). The *Hadith* concept is adopted from the muslim culture, and signifies a source of reliable and credible information.

Mohammadi et al. [181] investigated the problem on how to improve object and service discovery in IoT. An optimisation decision theory was considered adequate for the problem, that helps finding the optimal friend for an IoT object. This approach showed reduced resource consumption at the object level and simulation demonstrating pairing services' improvements in terms of average path length, degree distribution of the network and the number of links used.

Narang and Kar [182] considered a hybrid trust management framework to tackle the challenges of trust in multi-vendor heterogeneous SIoT environments. By applying a method called Probabilistic Neighbourhood Overlap, the authors tried to estimate the social tie-strengths between node connections. This method was applied over a social graph, generated first from the connections between IoT users, based on the interactions between the IoT objects. By fusing together human interactions and device to device interactions, the presented approach offered a trust management technique capable of limiting resource overheads, by combining a dynamic interaction-based assessment together with a graph-based static one. Lastly, Latif [183] proposed Con-Trust, a trust management method which considers the system's context when choosing and allocating jobs in SIoT. To achieve this, the trust model considered trust metrics such as job characteristics, object capabilities, honesty, and the impact of possible malicious behaviour.

I. DECENTRALISED LEDGERS FOR TRUST MANAGEMENT

While the literature survey at hand does not focus primarily on studies that use security techniques to achieve trust (e.g., trusted computing, software attestation), decentralised ledger technologies represent an exception. As Table 12 depicts, there is a high number of works in the literature, showcasing decentralised ledgers as a management solution for trust, through frameworks such as Hyperledger Fabric [185], [186], [190], [210] or Tendermint [205]. Consequently, it was considered adequate to include this domain in the survey, to pinpoint its place in the context of trust management.

The main use-case of decentralised ledgers, or Blockchain frameworks, mainly proposing to store and distribute data across peers in the network. While certain security properties are guaranteed by decentralised ledgers for data storage (e.g., authenticity, non-repudiation), there is a limited amount of works which analysed alternatives to data storage (e.g., distributed databases), or which provide performance measurements of Blockchain representing a better alternative to distributed data storage. An additional drawback of Blockchain, and how it is applied, is that authors do not take into consideration the fact that these ledgers mainly act as a *write-only* database, without the ability to delete past entries. Identity is an additional aspect covered by certain ledgers (e.g., Hyperledger Indy) to manage decentralised identities. Furthermore, identity is a crucial property of a TMM oriented network, helping in network access control and mitigating trust attacks (e.g., IMP).

There are two primary domains in which Blockchain is frequently applied: VANETs and WANETs or IoT networks. In both cases, edge nodes (e.g., sensor, vehicle) do not interact directly with the ledger. In [184] on the other hand, the authors proposed that vehicles to be Blockchain peers. Alternatively, the Blockchain network is constructed at the fog level, meaning that a gateway middleware handles the sensor-to-ledger communication in the case of WANET, and RSUs in the case of VANETs. In both domains, the focus is put on secure information sharing across the network. The shared information ranges from trust metrics [184], [185], trust or reputation values [186], [187], [188], [189], and blacklisting decisions for malicious or un-trustworthy node identification [190], [191], [192], [193].

Another problem solved with decentralised ledgers is secure sensor localisation. Goyat et al. [194] developed a trust-based sensor localisation algorithm that takes advantage of a ledger to enable beacon nodes to update their trust values. Additionally, a proof-of-stake is considered for consensus and block updates.

Mershad et al. [195] proposed a consensus mechanism titled Proof of Accumulated Trust, where VANET RSUs are dynamically elected as miners based on their accumulated trust value. The problem of consensus from a perspective of trust was also addressed by [196]. In this approach, consensus candidates are required to check the trust levels of other elected candidates to determine reciprocal trustworthiness. Jiang et al. [197] introduced a reputation-driven consensus model for Blockchain, meant to eliminate abnormal (e.g., untrustworthy) members that participate in the consensus process. Ultimately, the scope of the work is to reduce the probability that malicious individuals become trusted nodes. Several other works offered different possibilities on including trust in consensus and proposed a proof-of-x [198], [199].

J. QUANTITATIVE OVERVIEW

Nine TMM categories were identified, from which eight target trust modelling, and one trust management (e.g., Section VI-I on decentralised ledgers). As depicted in Figure 3, the most frequently seen approaches on solving trust modelling problems are Bayesian theory and statistical models, followed by ML. Even if uncertainty-based

TABLE 12. Overview of decentralised ledgers methods for trust management. (✓- considered, ✗- not considered, ∼ - partially considered.)

Source	Domain	Description	Resistant against	C1	C2	C3
[185]	VANET	TMM with Blockchain to share trust metrics in VANET.	N/A	✗	✓	✗
[186]	VANET	Decentralized ledger based on Hyperledger Fabric for storing and sharing trust values in a VANET environment.	N/A	✗	✓	✗
[187]	WSN	Decentralized ledger based on Hyperledger Fabric used in conjunction with the Beta reputation system for secure data storage regarding blacklisted nodes.	GEN	∼	✗	∼
[188]	VANET	Consortium Blockchain for storage and data sharing between Road Side Units (RSUs) in the VANET environment.	N/A	✗	✓	∼
[189]	VANET	Distributed storage for trust values computed with a trust model based on Bayesian inference.	GEN	✗	✓	✗
[190]	IoT	Data sharing using smart contracts for a similarity-based trust model.	OO, CL	∼	✗	∼
[191]	VANET	Trust evaluation using a Hidden Markov model for malicious node identification, with a Hyperledger based storage.	GEN	∼	✓	✗
[192]	VANET	Information sharing between vehicles about untrusted/malicious vehicles using a Decentralized ledger.	BH	✗	✓	∼
[193]	VANET	Decentralised distribution of information regarding blacklisted nodes using Blockchain technology in VANETs.	BM, SYB	✓	✗	∼
[194]	VANET	Anonymous malicious vehicle identification trough trust management and RSU-based Blockchain.	SYB, SB, IMP	✓	✓	✓
[195]	WSN	Trust-based sensor localisation algorithm on top of a Blockchain infrastructure.	SB, SYB, BM	✓	✓	✓
[196]	VANET	Consensus protocol established on a proof of accumulated trust.	GEN	✓	✓	✓
[197]	IoT	Consensus protocol leveraging trustful interactions and fusion for collaborated learning.	GEN	✓	✓	✓
[198]	IoT	Extended Practical Byzantine Fault Tolerance with a reputation score. Possible consensus solution against electing malicious nodes.	N/A	✗	✓	✓
[199]	IoT	Powered based Proof of Work (PoW) Blockchain with TOPSIS model for trust evaluation.	SYB, IMP, BM	✓	✓	✓
[200]	VANET	Trust management system based on blockchain, to assure authenticity of transmitted messages.	BM, MITM	✓	✓	∼
[201]	VANET	Blockchain-based trust management solution for anonymous region cloaking with a Dirichlet distribution-based trust model.	BM, OO, SYB, WW	✓	✓	✓
[202]	IoT	Decentralized trusted platform for edge computing meant to efficiently distribute tasks for IoT services.	N/A	✗	✓	✗
[203]	VANET	Trust management technique with local and global consensus mechanisms for VANET events.	N/A	✗	✓	✗
[204]	MANET	Secure caching framework using collaborative TMM based on Bayesian inference and DST.	OO	✓	✓	✓
[205]	IoT	Trust management for resource constrained sensors using Blockchain at fog level.	BM	∼	✓	∼
[206]	VANET	Reputation system built on top of a Decentralized ledger using the Tendermint Blockchain.	N/A	✗	✓	✗
[207]	VANET	A trust management approach leveraging Blockchain to record trust values, and k-anonymity for enhance vehicle privacy protection.	BM, OO	✓	✓	✓
[208]	VANET	Blockchain-base trust management solution to assure data consistency regarding un-cooperative vehicles.	MITM, SB, CL	✓	✓	✓
[209]	VANET	Weighted average trust model built on top of Blockchain infrastructure.	BM, SB	✗	∼	∼
[210]	IoT	Decentralised IoT framework built on a permissioned Blockchain with a intrusion tolerant system.	GEN	✗	✓	✗
[211]	IoT	Decentralised dynamic trust evaluation model under a Blockchain network.	OO, SYB, WW, SB	✓	✓	✓

frameworks such as DST or SL are suited for trust modelling, in the time frame considered their popularity is lower in comparison to Bayesian models or ML. As for trust management, decentralised ledgers or Blockchain technology

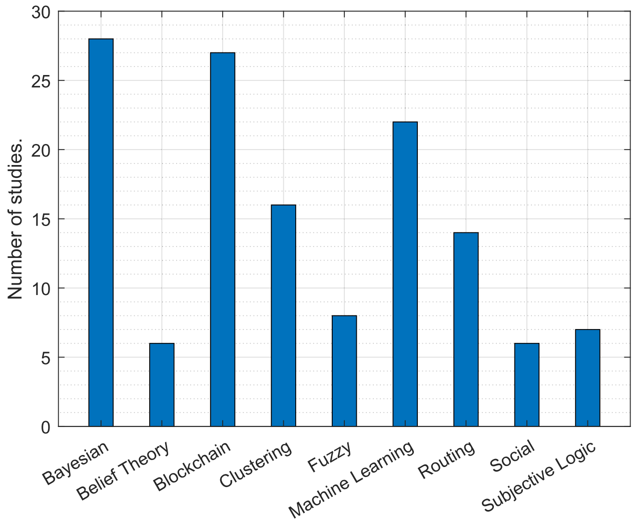

FIGURE 3. TMM categories with the total number of studies reviewed.

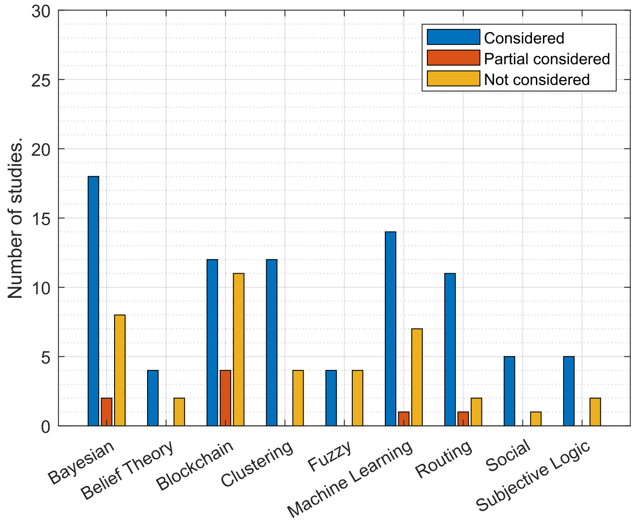

FIGURE 4. C1 evaluation index study distribution.

is frequently leveraged along a trust model to store and distribute trust related information. For the first comparison index C1, in Figure 4 it can be seen that 81 primary studies offer an experimental comparison with the state-of-the-art, while 8 only partially address this index, and 44 do not consider this criteria in validating their proposed approach.

In Figure 5 C2 is displayed. Here, the majority of the reviewed studies, with a total of 115, do conduct performance measurements to demonstrate the feasibility of their solution. While it is considered a general requirement for an experimental assessment, the difference between C1 and C2 may hold the observation from Gómez Mármol and Martínez Pérez [13] from over ten years ago, suggesting a high number of studies offering experimental measurements that are focused specifically on their method, lacking concrete comparison to other works.

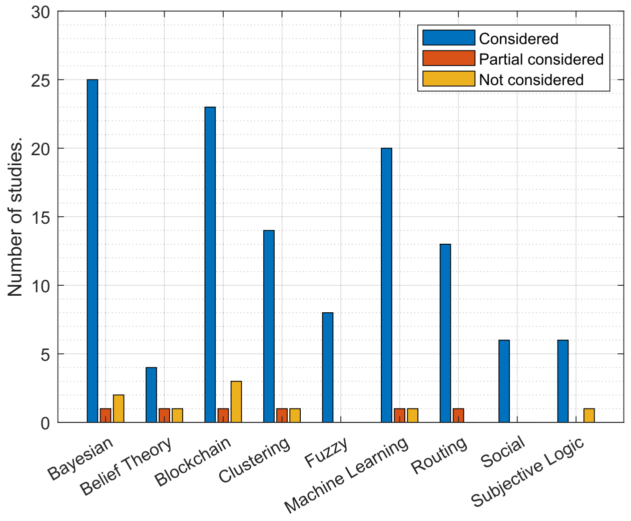

FIGURE 5. C2 evaluation index study distribution.

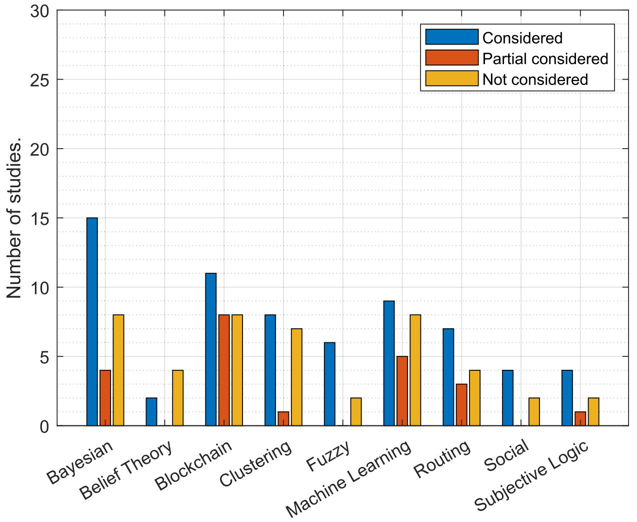

FIGURE 6. C3 evaluation index study distribution.

From Figure 6, where the third index C3 is presented, we can draw the following conclusion. Since TMM offers an additional layer of security over the existing communication infrastructure, with or without secure communication channels, C3 intends to quantify the number of papers that offer concrete experimentation against TMM attacks. Otherwise, if these measurements or analysis is not provided, it is challenging to evaluate the behaviour of the study solution against threats. 64 studies conducted an experimental assessment against TMM attacks, while 37 did not consider it, as can be seen in Figure 6. Partially considered, in this context means that the authors addressed this index but not entirely, describing generic attacks, or only tackling small subset of TMM attacks. This aspect is emphasised by Figure 7, where the most frequently reported attacks are displayed. From this, it can be concluded that there is a high number of papers which do not mention any trust attacks. This number differs

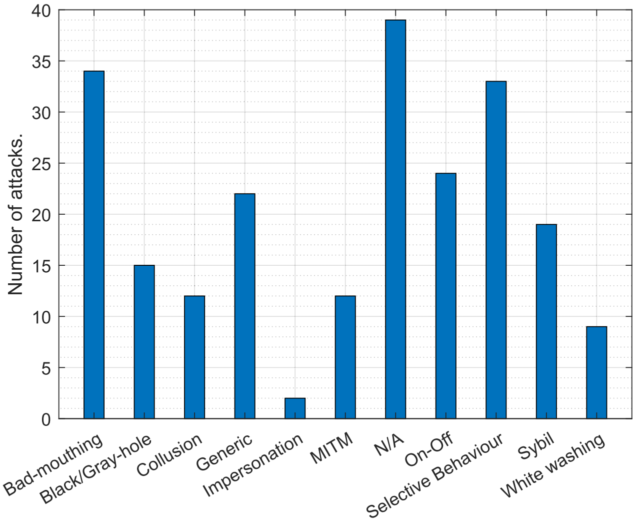

FIGURE 7. Most frequently reported trust attacks in the analysed studies.

from the result from C3 because of the presence of the Generic attack.

In Figure 7, it can be observed that the most frequently considered trust attacks are Selective Behaviour and Bad-mouthing/Ballot stuffing, followed by On-Off and Sybil. On the opposite side, the least considered trust attacks are Impersonation, White washing and Collusion. The reason why an Impersonation attack is not addressed may reside in its similarity with the Sybil attack. In a Sybil attack, an attacker claims or steals the identities of multiple nodes to propagate false information in the network. For Impersonation, the attack is limited in comparison to a specific target. The same parallel can be made between Sybil and Collusion, since the latter entails a group of malicious nodes publishing altered information to decrease the trust level in legitimate nodes.

K. PERFORMANCE METRICS

Comparison criteria C2 outlines for each primary study the availability of model experiments, and performance analysis. To better evaluate the efficiency of the primary studies, we have extracted in Table 13 a series of performance metrics. Here, the metrics considered are: detection delay, accuracy (ACC), False positive rate (FPR), False negative rate (FNR), True positive rate (TPR) (or recall), True negative rate (TNR) (or specificity), and precision (PRC). We would like to highlight that not all primary studies are mentioned in Table 13, but only those addressing the considered metrics. Moreover, the metrics are relevant to primary studies which target the detection of untrusted nodes (e.g., detecting trust threats, malicious nodes), while they could be less relevant for methods which leverage trust for routing. Along these metrics, the platform on which the evaluation was conducted is mentioned. The performance metrics outlined in Table 13 were identified according to the following equations:

$$
\begin{aligned}
ACC &= \frac{TP + TN}{TP + TN + FP + FN}, \\
FPR &= \frac{FP}{FP + TN} = 1 - TNR, \\
FNR &= \frac{FN}{FN + TP}, \\
TPR &= \frac{TP}{TP + FN}, \\
TNR &= \frac{TN}{TN + FP}, \\
PRC &= \frac{TP}{TP + FP}.
\end{aligned}
$$

The results obtained for each metric in Table 13 are offered as values in the range of 0 to 100. Furthermore, since there were cases in which multiple experiments were conducted covering the same metric, we present the results as an interval of two values, where the first value represents the minimum value obtained, and the second represents the maximum. Primary studies that did not define and measure the performance metrics regarding the equations above, were excluded. From a total number of 133 primary studies, 44 papers measured at least one performance metric. While these metrics are fundamental in evaluating the effectiveness of a model, a high number of studies do not address them. This issue was pointed out by Gómez Mármol and Martínez Pérez [13] as well, and it appears that the phenomenon still persists in the literature. However, even if not addressing these performance metrics, studies tend to measure computational overheads and complexities, communication delays and overhead, with several model specific measurements. While these experiments can represent a basis for model validation, objective metrics must represent a requirement.

VII. DISCUSSION

We orient our discussion towards two distinct directions. First, we discuss and identify the most suited TMM approaches to solve trust issues in DWN. Secondly, we provide the answers to the RQs raised in this paper.

The research literature of TMM is at an inflection point. As outlined in the quantitative overview, more precisely in Figure 3, a part of the primary studies analysed adopted techniques such a decentralised ledgers and machine learning to solve TMM issues. While we can not deny the innovation brought up by these methods, it is to state that their applicability can be misleading. Decentralised ledgers (or Blockchains) are frequently employed due to their intrinsic cryptographic properties, disregarding the DWN communication and hardware requirements. They are proposed as a solution since the ledger can act as a write-only tamper-proof database. While this is true, alternative storage options (e.g., distributed databases, look-up tables) are not considered in the literature. In TMM a node's identity should be represented by its trust values from a group of peers, and can be accompanied by other cryptographic means.

TABLE 13. Overview of TMM approaches' performance metrics.

Source	Platform	Detection delay [s]	ACC [%]	FPR [%]	FNR [%]	TPR [%]	TNR [%]	PRC
Bayesian and statistical models								
[51]	Veins	-	-	-	-	[90.0-100]	[50.0-100]	-
[52]	NS-3	-	97.3	-	-	-	-	-
[53]	NS-2	0.7	[50-80]	[0.0-30.0]	-	-	-	-
[57]	Matlab	-	[86.0-96.2]	[2.0-10.0]	-	-	-	-
[60]	OMNet++	-	[80.0-90.0]	[7.0-18.0]	-	-	-	-
[62]	python	-	100	-	-	-	-	-
[63]	Matlab	-	[50-100]	-	-	-	-	-
[71]	NetLogo	-	90.0	-	-	-	-	-
[72]	OMNet++, SUMO, Veins	-	-	-	-	[89.0-91.0]	-	[88.0-90.0]
[78]	NS-2	-	-	[0.0-14.0]	-	[89.0-94.0]	-	-
[189]	python	-	[85.2-94.8]	-	-	-	-	[84.0-90.0]
[194]	Veins, OMNet++, SUMO	-	-	[0.5-3.0]	-	[83.0-95.0]	-	[90.0-96.0]
[208]	NS-3	-	95	-	-	-	-	-
[201]	Java	-	[90.3-95.6]	-	-	-	-	
[195]	Matlab	-	[98.0-83.0]	[2.0-18.0]	[1.5-17.0]	-	-	-
Clustering-based models								
[86]	Matlab	-	-	[0.0-3.0]	[0.0-2.0]	-	-	-
[88]	NS-2	-	[70.0-90.0]	-	-	-	-	-
[89]	Veins	-	[95.8-84.7]	-	-	[74.0-100]	-	-
[90]	python	-	[81.0-96.0]	-	-	-	-	-
[91]	python	-	95.0	[9.0-16.0]	-	-	-	-
[94]	NS-3	-	[71.0-98.0]	[2.0-4.0]	[2.9-3.6]	[84.0-87.0]	-	[97.0-99.0]
[100]	python	-	95	[7.0-16.0]	[3.0-4.0]	-	-	86.67
Routing-based models								
[111]	NS-2	-	-	[10.0-20.0]	-	[60.0-90.0]	-	-
[113]	Matlab	-	[90.0-98.0]	-	-	-	-	-
[116]	Matlab	-	99.0	[4.0-5.0]	-	-	-	-
[117]	Matlab	-	[85.0-98.0]	-	-	-	-	
[121]	Matlab	-	90.0	1.0	-	96.0	-	95.0
Subjective logic models								
[145]	NS-3	-	[79.6-92.5]	0.0	[22.0-90.0]	-	-	-
[146]	Matlab	[0.001-0.009]	[86.0-96.0]	-	-	-	-	-
[147]	Contiki OS, Cooja	-	[88.0-98.0]	[2.0-0.0]	[0.0-4.0]	-	-	-
Fuzzy logic models								
[152]	MOVE, NS-2, SUMO	-	[90.0-99.0]	6.3	-	[85.0-95.0]	-	[85.0-97.0]
[153]	Matlab	-	96.0	-	-	-	-	-
[154]	NS-3	-	[75.0-100]	-	-	-	-	-
[155]	Matlab	-	-	[9.0-11.0], [10.5-14.0]	-	88.0, 92.2, 82.3, 90.0	-	-

TABLE 13. ***(Continued.)*** **Overview of TMM approaches' performance metrics.**

Machine learning models								
[158]	SUMO	-	[52.0-97.0]	-	-	-	-	-
[159]	Desktop	-	[75.0-99.0]	-	-	[78.0-99.0]	-	[75.0-99.0]
[161]	python	-	[81.0-98.3]	-	-	-	-	-
[162]	Desktop	-	[84.0-100]	-	-	-	-	-
[164]	Matlab	-	[60.0-98.0]	-	-	-	-	-
[166]	NS-2	-	[87.0-90.0]	-	-	[96.0-84.0]	-	[84.0-93.0]
[167]	COOJA	-	[92.0-98.0], [89.0-99.0]	[1.0-73.0]	-	-	[60.0-100]	[60.0-100]
[169]	Tmote Sky	-	100	-	-	-	-	-
[170]	ONE sim	[0.003-0.006]	-	[10.5-15.0]	-	-	-	-
[171]	Matlab	-	[95.0-100]	-	-	91.0	-	92.0

Machine learning-based trust models are generally applicable on DWN assisted by external cloud services. Exception exists, where these models can run locally, such as VANETs, since the underlying hardware is considered capable of handling allocated tasks. In computationally restricted environments (e.g., WSN, IoT, MANET), which require fast computations with low resource overhead, Bayesian models, Fuzzy Theory, Subjective logic or Belief Theory are the most suited options. These modelling techniques follow the initial philosophy on which the concept of TMM was built, being capable to handle uncertain information that can contain false information generated by possibly misbehaving neighbours.

In continuation, we proceed with answering the raised RQs. Our survey raised five RQs. The current section discusses and provides answers to each question. The RQs intended to cover general aspects of TMM, ranging from the motivation and advantages behind TMM techniques, to security implications and gaps in model validation.

RQ 1: *What are the advantages, motivation, and objectives behind TMM?*

Answer: TMM is applied in ad-hoc DWNs to encourage cooperation between network members, and to punish disruptive behaviour manifested by malicious nodes. TMM offers an additional layer of security over the existing communication channels by constructing a trust network where each network member is trusted to a degree by other members. In a trust network, trust relationships are formed based on first (e.g., direct trust) and second hand (e.g., indirect trust) interactions between the network members. Moreover, from Section III and VI we can conclude that TMM techniques are applied in routing, for finding the most trustworthy path; in clustering to build and maintain trust groups, or in intrusion detection to eliminate untrustworthy nodes.

RQ 2: *What are the most frequently applied TMM methods?*

Answer: In the time frame considered, our analysis points out that the most applied trust modelling techniques are models based on Bayesian theory and Statistics, followed by ML. This is supported by the results in Figure 4. Furthermore, we observed an increased number of papers adopting decentralised ledgers as a trust management approach in conjunction with a trust model (e.g., Section VI-I). Even so, methods offering the capability to reason under uncertainty (e.g., DST, SL), represent a suitable solution for trust modelling. More insights are offered in Section VI-J. Along trust modelling, there are approaches that build DWN functionalities (e.g., routing, clustering) that leverage trust values as their core reasoning mechanism. For example, in the case of routing, the most trustworthy paths are selected to forward packets, while for clustering, the node trusted by a larger group of nodes is elected as CH.

RQ 3: *What are the core components of a generic TMM technique?*

Answer: The work at hand addresses this RQ in two ways. First, it synthesises TMM terminology under the form of an ontology in Section IV-A. Secondly, it defines a general trust model in Section IV-B, outlining the main components that were identified across primary studies.

RQ 4: *What is the security validation degree undertaken by studies?*

Answer: Our survey provides an answer to this RQ in two ways. First, for each study analysed, the survey provides the trust attacks considered, together with the degree of validation against identified threats in the study experimental assessment (i.e., by using C3 comparison index). From C3 we reason that approximately 50% of studies conduct security experiments against trust threats. On the other hand, we found that 39 studies out of 133 do not consider this aspect. Additionally, we observed the trend in the literature for experimental validation in controlled simulated environments, as shown in Figure 5. This raises the inquiry on the plausibility of TMM security and its application in real life environments.

RQ 5: *What are the security issues addressed by TMM in the domain of DWNs?*

Answer: It is noteworthy to mention again that the current study was restricted to a period of three years (2020-2022). Therefore, insights in the past works were obtained from thoroughly researching past published surveys. Even if there is a high diversity in TMM, the analysis conducted brought forth several points brought up in past surveys. First, as shown in Section VI-J, there is a gap in the model validation. We consider that TMM approaches require a strong experimental analysis in security and resistance against TMM specific attacks. A second observation is that most TMM methods are validated through simulation as mentioned in RQ 4. Rarely, a model is deployed over concrete hardware in a closer to reality environment. While simulations can provide useful understanding of the model behaviour, the literature lacks deployment of TMM methods over real systems.

VIII. OPEN RESEARCH ISSUES

The work at hand surveyed the concept of trust from the TMM perspective. Ultimately, the main scope of TMM is to build trust relationships in a group of nodes, and to ensure a degree of security. The present systematic literature analysis brought up several insights regarding the current research state of TMM.

First, to improve the quality and real-life feasibility of TMM methods, researchers must focus in the future on thorough and comparable experimental assessments, with application to real life environments.

Secondly, while conducting our literature review, we observed a vast amount of environments in which experiments were conducted, and a similar diversity in types of experiments and measurements. As Table 13 showcases, we can observe that the majority of primary studies adopted a simulation environment for model validation purposes. Even if Table 13 does not encapsulate all the surveyed primary studies, the trend persists across the literature. At a first glance over the TMM literature this may not impose a problem, since a reader may discover a minor sight of the whole literature. This problem is more significant since the trend persists across the literature, raising the questioning on the applicability of TMM techniques.

Finally, the next major milestone that must be reached by the scientific community of TMM, is to pursue the deployment of these approaches in real-life systems and scenarios. This aspect is crucial, since we can not rely only on simulation results to evaluate the effectiveness of a TMM method. After deploying a TMM, the next hiccup that must be overcome is translating the simulation validation process conducted offline, into the real environment. This does not only include performance analysis, but additionally implementing and testing trust-based attacks. Only by going in this direction, we can objectively evaluate the applicability and feasibility of TMM methods and their contribution to system security and decision making.

IX. CONCLUSION

The paper at hand offers a thorough literature survey on the most recent TMM approaches in ad-hoc DWNs. The survey covers over 130 research papers published in the time period from 2020 to 2022. The studies subjected to the review were identified, screened, filtered and analysed based on a RP. The protocol was designed to provide a clear and concise view for the reader over the review process execution. Prior to the comparison analysis, we introduced and generalised the most common terminology of TMM techniques as an ontology, define the building blocks of a trust model, and pinpoint most common TMM threats.

In the conducted analysis, we focused on comparing TMM techniques from three distinct stands, enabling assessment of the level of validation that was undertaken to validate each study. As such, three comparison indexes were defined. The first index (C1) points out if the efficiency of a study was validated against known methods available in the literature. The second index (C2) considers the aspect of performance experimentation, while the third index (C3) undertakes the factor of evaluation against TMM threats.

By taking into account the gaps raised in the related works, the research questions raised in this paper, and the comparison with the quantitative overview, the following conclusions can be drawn. The major gap in the literature in the time frame considered remains mainly in model evaluation against trust attacks and threats. This aspect makes it challenging to judge the model's viability and efficiency in contrast with other related techniques. Additionally, we have observed that a higher importance is put in research papers on experimental assessments, with or without a comparison against state-of-the-art. This aspect in conjunction with the number of modelling techniques available to tackle the problem of trust, makes it problematic to assess and compare TMM methods if they do not have similar approaches.

ACKNOWLEDGMENT

This work is supported by the OPEVA project that has received funding within the Key Digital Technologies Joint Undertaking (KDT JU) from the European Union's Horizon Europe Programme under grant agreement No 101097267 and was co-funded by the Swiss State Secretariat for Education, Research and Innovation (SERI) and the Innosuisse—Swiss Innovation Agency. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or KDT JU. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

[1] M. Frikha, *Ad Hoc Networks*, 1st ed. Hoboken, NJ, USA: Wiley, Feb. 2013.

[2] G. Khayat, C. X. Mavromoustakis, G. Mastorakis, J. M. Batalla, H. Maalouf, and E. Pallis, "VANET clustering based on weighted trusted cluster head selection," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 623–628. [Online]. Available: https://ieeexplore.ieee.org/document/9148339/

[3] R. Di Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks—A survey," *Comput. Commun.*, vol. 51, pp. 1–20, Sep. 2014.

[4] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, Dec. 2015.

[5] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011. [Online]. Available: http://ieeexplore.ieee.org/document/5604602/

[6] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Comput. Surv.*, vol. 48, no. 2, pp. 1–40, Nov. 2015, doi: 10.1145/2815595.

[7] M. Mejia, N. Peña, J. L. Muñoz, and O. Esparza, "A review of trust modeling in ad hoc networks," *Internet Res.*, vol. 19, no. 1, pp. 88–104, Jan. 2009.

[8] D. Gambetta, "Can we trust trust?" in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed. Oxford, U.K.: Blackwell, 1988, pp. 213–237.

[9] H. Li and M. Singhal, "Trust management in distributed systems," *Computer*, vol. 40, no. 2, pp. 45–53, Feb. 2007. [Online]. Available: http://ieeexplore.ieee.org/document/4085622/

[10] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: A survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, Mar. 2021. [Online]. Available: https://www.mdpi.com/2624-831X/2/1/9

[11] C. Marche and M. Nitti, "Can we trust trust management systems?" *IoT*, vol. 3, no. 2, pp. 262–272, Mar. 2022. [Online]. Available: https://www.mdpi.com/2624-831X/3/2/15

[12] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi, "Decentralized trust management: Risk analysis and trust aggregation," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–33, Jan. 2021, doi: 10.1145/3362168.

[13] F. Gómez Mármol and G. Martínez Pérez, "Trust and reputation models comparison," *Internet Res.*, vol. 21, no. 2, pp. 138–153, Jan. 2011.

[14] D. M. Mena, I. Papapanagiotou, and B. Yang, "Internet of Things: Survey on security," *Inf. Secur. J.*, vol. 27, no. 3, pp. 162–182, 2018.

[15] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "Iot-based smart cities: A survey," in *Proc. IEEE 16th Int. Conf. Environ. Electr. Eng.*, Jun. 2016, pp. 1–6.

[16] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[17] V. P. Kour and S. Arora, "Recent developments of the Internet of Things in agriculture: A survey," *IEEE Access*, vol. 8, pp. 129924–129957, 2020.

[18] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, Apr. 2019.

[19] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *J. Netw. Comput. Appl.*, vol. 97, pp. 48–65, Nov. 2017.

[20] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Netw.*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[21] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.

[22] K. Thirunarayan, P. Anantharam, C. Henson, and A. Sheth, "Comparative trust management with applications: Bayesian approaches emphasis," *Future Gener. Comput. Syst.*, vol. 31, pp. 182–199, Feb. 2014.

[23] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[24] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in Internet of Things systems," *Comput. Commun.*, vol. 97, pp. 1–14, Jan. 2017.

[25] F. Amin, A. Ahmad, and G. S. Choi, "Towards trust and friendliness approaches in the social Internet of Things," *Appl. Sci.*, vol. 9, no. 1, p. 166, Jan. 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/1/166

[26] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. Khan, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, Art. no. 102409.

[27] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy Internet of Things: A survey on trust management applications and schemes," *Comput. Commun.*, vol. 160, pp. 475–493, Jul. 2020.

[28] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social Internet of Things: A taxonomy, open issues, and challenges," *Comput. Commun.*, vol. 150, pp. 13–46, Jan. 2020.

[29] S. Ayed, L. Chaari, and A. Fares, "A survey on trust management for WBAN: Investigations and future directions," *Sensors*, vol. 20, no. 21, p. 6041, Oct. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/21/6041

[30] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A survey of trust management in the Internet of Vehicles," *Electronics*, vol. 10, no. 18, p. 2223, Sep. 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/18/2223

[31] K. Mannix, A. Gorey, D. O'Shea, and T. Newe, "Sensor network environments: A review of the attacks and trust management models for securing them," *J. Sensor Actuator Netw.*, vol. 11, no. 3, p. 43, Aug. 2022. [Online]. Available: https://www.mdpi.com/2224-2708/11/3/43

[32] C. Marche, L. Atzori, V. Pilloni, and M. Nitti, "How to exploit the social Internet of Things: Query generation model and device profiles' dataset," *Comput. Netw.*, vol. 174, Jun. 2020, Art. no. 107248.

[33] K. Thirunarayan and P. Anantharam, "Trust networks: Interpersonal, sensor, and social," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, May 2011, pp. 13–21. [Online]. Available: http://ieeexplore.ieee.org/document/5928659/

[34] N. F. Noy and D. L. McGuinness, "Ontology development 101: A guide to creating your first ontology," Stanford Knowl. Syst. Lab., Stanford Med. Inform., Tech. Rep. KSL-01-05 and SMI-2001-0880, 2001. [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=FE08ALAAAAAJ&citation_for_view=FE08ALAAAAAJ:u5HHmVD_uO8C

[35] X. Liu, S. Tang, Q. Huang, and Z. Yu, "An ontology-based approach to automated trust negotiation," *Comput. Standards Interfaces*, vol. 36, no. 1, pp. 219–230, Nov. 2013.

[36] N. Karthik and V. S. Ananthanarayana, "An ontology based trust framework for sensor-driven pervasive environment," in *Proc. Asia Model. Symp. (AMS)*, Dec. 2017, pp. 147–152. [Online]. Available: https://ieeexplore.ieee.org/document/8424321/

[37] M. Taherian, R. Jalili, and M. Amini, "PTO: A trust ontology for pervasive environments," in *Proc. 22nd Int. Conf. Adv. Inf. Netw. Appl.-Workshops*, 2008, pp. 301–306.

[38] F. K. Hussain, E. Chang, and T. S. Dillon, "Trust ontology for service-oriented environment," in *Proc. IEEE Int. Conf. Comput. Syst. Appl.*, Mar. 2006, pp. 320–325.

[39] W. Sherchan, S. Nepal, J. Hunklinger, and A. Bouguettaya, "A trust ontology for semantic services," in *Proc. IEEE Int. Conf. Services Comput.*, Jul. 2010, pp. 313–320.

[40] O. Jules, A. Hafid, and M. A. Serhani, "Bayesian network, and probabilistic ontology driven trust model for SLA management of cloud services," in *Proc. IEEE 3rd Int. Conf. Cloud Netw. (CloudNet)*, Oct. 2014, pp. 77–83.

[41] L. Viljanen, "Towards an ontology of trust," in *Proc. Int. Conf. Trust, Privacy Security Digital Business*, 2005, pp. 175–184.

[42] J. Huang and M. S. Fox, "An ontology of trust: Formal semantics and transitivity," in *Proc. 8th Int. Conf. Electronic Commerce, New e-Commerce, Innov. Conquering Current Barriers, Obstacles Limitations Conducting Successful Bus. Internet*, New York, NY, USA, 2006, p. 259.

[43] A. Oltramari and J.-H. Cho, "ComTrustO: Composite trust-based ontology framework for information and decision fusion," in *Proc. 18th Int. Conf. Inf. Fusion (Fusion)*, 2015, pp. 542–549.

[44] G. Amaral, T. P. Sales, G. Guizzardi, and D. Porello, "Towards a reference ontology of trust," in *Proc. OTM Confederated Int. Conf. 'Move Meaningful Internet Syst.'*, 2019, pp. 3–21.

[45] C. Castelfranchi, R. Falcone, and E. Lorini, "A non-reductionist approach to trust," in *Computing With Social Trust*, J. Golbeck, Ed. London, U.K.: Springer, 2009, pp. 45–72, doi: 10.1007/978-1-84800-356-9_3.

[46] D. H. McKnight and N. L. Chervany, "The meanings of trust," Carlson School Manage., Univ. Minnesota, Tech. Rep., 1996.

[47] A. Josang, *Subjective Logic*, vol. 3. Berlin, Germany: Springer, 2016.

[48] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, 2007.

[49] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007.

[50] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: An anti-attack trust management scheme in VANET," *IEEE Access*, vol. 8, pp. 21077–21090, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8960345/

[51] G. Chen, F. Zeng, J. Zhang, T. Lu, J. Shen, and W. Shu, "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems," *Comput. Netw.*, vol. 190, May 2021, Art. no. 107952.

[52] A. R. Rajeswari, S. Ganapathy, K. Kulothungan, and A. Kannan, "An efficient trust-based secure energy-aware clustering to mitigate trust distortion attack in mobile ad-hoc network," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 13, p. e6223, Jul. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/cpe.6223

[53] Y. Fu and Z. He, "Bayesian-inference-based sliding window trust model against probabilistic SSDF attack in cognitive radio networks," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1764–1775, Jun. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8822487/

[54] H. Gao, C. Liu, Y. Yin, Y. Xu, and Y. Li, "A hybrid approach to trust node assessment and management for VANETs cooperative data communication: Historical interaction perspective," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16504–16513, Sep. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9629245/

[55] A. Saidi, "Trust evaluation method for wireless sensor networks based on behavioral similarity and similarity coefficient," in *Proc. Int. Conf. Netw. Adv. Syst. (ICNAS)*, Oct. 2021, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9628892/

[56] Z. Teng, C. Du, M. Li, H. Zhang, and W. Zhu, "A wormhole attack detection algorithm integrated with the node trust optimization model in WSNs," *IEEE Sensors J.*, vol. 22, no. 7, pp. 7361–7370, Apr. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9716928/

[57] N. V. Abhishek and T. J. Lim, "Trust-based adversary detection in edge computing assisted vehicular networks," *J. Commun. Netw.*, vol. 24, no. 4, pp. 451–462, Aug. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9851614/

[58] J. Ren and T. Qin, "A novel multidimensional trust evaluation and fusion mechanism in fog-based Internet of Things," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109354.

[59] K. N. Qureshi, A. Iftikhar, S. N. Bhatti, F. Piccialli, F. Giampaolo, and G. Jeon, "Trust management and evaluation for edge intelligence in the Internet of Things," *Eng. Appl. Artif. Intell.*, vol. 94, Sep. 2020, Art. no. 103756.

[60] F. Jabeen, Z. Khan, Z. Hamid, Z. Rehman, and A. Khan, "Adaptive and survivable trust management for Internet of Things systems," *IET Inf. Secur.*, vol. 15, no. 5, pp. 375–394, Sep. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1049/ise2.12029

[61] K. Kalkan and K. Rasmussen, "TruSD: Trust framework for service discovery among IoT devices," *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107318.

[62] G. Zhang, T. Wang, G. Wang, A. Liu, and W. Jia, "Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 7, Apr. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/cpe.5109

[63] D. Shehada, A. Gawanmeh, C. Y. Yeun, and M. Jamal Zemerly, "Fog-based distributed trust and reputation management system for Internet of Things," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8637–8646, Nov. 2022.

[64] I. U. Din, K. A. Awan, A. Almogren, and B.-S. Kim, "ShareTrust: Centralized trust management mechanism for trustworthy resource sharing in industrial Internet of Things," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 108013.

[65] A. Anwar, T. Halabi, and M. Zulkernine, "A coalitional security game against data integrity attacks in autonomous vehicle networks," *Veh. Commun.*, vol. 37, Oct. 2022, Art. no. 100517.

[66] H. Yahyaoui, Z. Maamar, M. Al-Khafajiy, and H. Al-Hamadi, "Trust-based management in IoT federations," *Future Gener. Comput. Syst.*, vol. 136, pp. 182–192, Nov. 2022.

[67] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor-cloud system," *Future Gener. Comput. Syst.*, vol. 109, pp. 573–582, Aug. 2020.

[68] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2054–2062, Mar. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8769947/

[69] M. M. Arifeen, D. Bhakta, S. R. H. Remu, M. M. Islam, M. Mahmud, and M. S. Kaiser, "Hidden Markov model based trust management model for underwater wireless sensor networks," in *Proc. Int. Conf. Comput. Advancements*, New York, NY, USA, Jan. 2020, pp. 1–5, doi: 10.1145/3377049.3377054.

[70] W. Kong, X. Li, L. Hou, and Y. Li, "An efficient and credible multi-source trust fusion mechanism based on time decay for edge computing," *Electronics*, vol. 9, no. 3, p. 502, Mar. 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/3/502

[71] H. El-Sayed, S. Zeadally, M. Khan, and H. Alexander, "Edge-centric trust management in vehicular networks," *Microprocess. Microsyst.*, vol. 84, Jul. 2021, Art. no. 104271.

[72] Y. Ouyang, Z. Zeng, X. Li, T. Wang, and X. Liu, "A verifiable trust evaluation mechanism for ultra-reliable applications in 5G and beyond networks," *Comput. Standards Interfaces*, vol. 77, Aug. 2021, Art. no. 103519.

[73] A. Altaf, H. Abbas, F. Iqbal, F. A. Khan, S. Rubab, and A. Derhab, "Context-oriented trust computation model for industrial Internet of Things," *Comput. Electr. Eng.*, vol. 92, Jun. 2021, Art. no. 107123.

[74] C. Suraci, S. Pizzi, D. Garompolo, G. Araniti, A. Molinaro, and A. Iera, "Trusted and secured D2D-aided communications in 5G networks," *Ad Hoc Netw.*, vol. 114, Apr. 2021, Art. no. 102403.

[75] J. Guo, H. Wang, W. Liu, G. Huang, J. Gui, and S. Zhang, "A lightweight verifiable trust based data collection approach for sensor-cloud systems," *J. Syst. Archit.*, vol. 119, Oct. 2021, Art. no. 102219.

[76] S.-C. Arseni, B.-C. Chifor, M. Coca, M. Medvei, I. Bica, and I. Matei, "RESFIT: A reputation and security monitoring platform for IoT applications," *Electronics*, vol. 10, no. 15, p. 1840, Jul. 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/15/1840

[77] A. K. Fabi and S. M. Thampi, "A trust management framework using forest fire model to propagate emergency messages in the Internet of Vehicles (IoV)," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100404.

[78] J. M. Bernardo and A. F. Smith, *Bayesian Theory*, J. M. Bernardo and A. F. M. Smith, Eds. Hoboken, NJ, USA: Wiley, May 1994.

[79] L. Page, S. Brin, R. Motwani, and T. Winograd, "The PageRank citation ranking: Bringing order to the web," in *Proc. Web Conf. Comput. Sci., Math.*, Nov. 1999.

[80] J. B. MacQueen, "Some methods for classification and analysis of MultiVariate observations," in *Proc. 5th Berkeley Symp. Math. Statist. Probab.*, vol. 1, L. M. L. Cam and J. Neyman, Eds. Berkeley, CA, USA: Univ. California Press, 1967, pp. 281–297.

[81] J. P. Vert, K. Tsuda, and B. Schölkopf, "A primer on kernel methods," in *Kernel Methods in Computational Biology*. Cambridge, MA, USA: MIT Press, Aug. 2004, doi: 10.7551/mitpress/4057.003.0004.

[82] D. M. Endres and J. E. Schindelin, "A new metric for probability distributions," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1858–1860, Jul. 2003.

[83] J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 1, pp. 32–48, 1st Quart., 2005.

[84] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, and S. Khan, "StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks," *IEEE Access*, vol. 8, pp. 21159–21177, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8967094/

[85] A. Saidi, K. Benahmed, and N. Seddiki, "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks," *Ad Hoc Netw.*, vol. 106, Sep. 2020, Art. no. 102215.

[86] A. Amuthan and A. Arulmurugan, "Semi-Markov inspired hybrid trust prediction scheme for prolonging lifetime through reliable cluster head selection in WSNs," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 33, no. 8, pp. 936–946, Oct. 2021.

[87] N. Veeraiah, O. Ibrahim Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani, "Trust aware secure energy efficient hybrid protocol for MANET," *IEEE Access*, vol. 9, pp. 120996–121005, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9525105/

[88] J. Montenegro, C. Iza, and M. A. Igartua, "Detection of position falsification attacks in VANETs applying trust model and machine learning," in *Proc. 17th ACM Symp. Perform. Eval. Wireless Ad Hoc, Sensor, Ubiquitous Netw.*, New York, NY, USA, Nov. 2020, pp. 9–16, doi: 10.1145/3416011.3424757.

[89] Z. Ma, L. Liu, and W. Meng, "Towards multiple-mix-attack detection via consensus-based trust management in IoT networks," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101898.

[90] L. Liu, X. Xu, Y. Liu, Z. Ma, and J. Peng, "A detection framework against CPMA attack based on trust evaluation and machine learning in IoT network," *IEEE Internet Things J.*, vol. 8, no. 20, pp. 15249–15258, Oct. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9324748/

[91] L. Yang, Y. Lu, S. X. Yang, T. Guo, and Z. Liang, "A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4837–4847, Jul. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9177296/

[92] M. Padmaa, T. Jayasankar, S. Venkatraman, A. K. Dutta, D. Gupta, S. Shamshirband, and J. P. C. Rodrigues, "Oppositional chaos game optimization based clustering with trust based data transmission protocol for intelligent IoT edge systems," *J. Parallel Distrib. Comput.*, vol. 164, pp. 142–151, Jun. 2022.

[93] C. Pedroso and A. Santos, "Dissemination control in dynamic data clustering for dense IIoT against false data injection attack," *Int. J. Netw. Manag.*, vol. 32, no. 5, Sep. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/nem.2201

[94] L. Guo, Y. Zhu, H. Yang, Y. Luo, L. Sun, and X. Zheng, "A *k*-nearest neighbor query method based on trust and location privacy protection," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 16, Jul. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/cpe.5766

[95] H. Farman, A. Khalil, N. Ahmad, W. Albattah, M. A. Khan, and M. Islam, "A privacy preserved, trust relationship (PTR) model for Internet of Vehicles," *Electronics*, vol. 10, no. 24, p. 3105, Dec. 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/24/3105

[96] C. Boudagdigue, A. Benslimane, A. Kobbane, and J. Liu, "Trust management in industrial Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3667–3682, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9099265/

[97] A. Roy and S. Madria, "Distributed incentive-based secured traffic monitoring in VANETs," in *Proc. 21st IEEE Int. Conf. Mobile Data Manag. (MDM)*, Jun. 2020, pp. 49–58. [Online]. Available: https://ieeexplore.ieee.org/document/9162241/

[98] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Trusted object framework (TOF): A clustering reputation-based approach using edge computing for sharing resources among IoT smart objects," *Comput. Electr. Eng.*, vol. 96, Dec. 2021, Art. no. 107568.

[99] R. B. Kagade and S. Jayagopalan, "Optimization assisted deep learning based intrusion detection system in wireless sensor network with two-tier trust evaluation," *Int. J. Netw. Manag.*, vol. 32, no. 4, p. e2196, Jul. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/nem.2196

[100] W. Kong, X. Li, L. Hou, J. Yuan, Y. Gao, and S. Yu, "A reliable and efficient task offloading strategy based on multifeedback trust mechanism for IoT edge computing," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13927–13941, Aug. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9684518/

[101] V. Estivill-Castro, "Why so many clustering algorithms," *ACM SIGKDD Explor. Newslett.*, vol. 4, no. 1, pp. 65–75, Jun. 2002.

[102] S. C. Johnson, "Hierarchical clustering schemes," *Psychometrika*, vol. 32, no. 3, pp. 241–254, Sep. 1967.

[103] J. A. Hartigan and M. A. Wong, "Algorithm AS 136: A K-means clustering algorithm," *Appl. Statist.*, vol. 28, no. 1, p. 100, 1979.

[104] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," in *Proc. 2nd Int. Conf. Knowl. Discovery Data Mining*, 1996, pp. 226–231.

[105] J. C. Bezdek, R. Ehrlich, and W. Full, "FCM: The fuzzy c-means clustering algorithm," *Comput. Geosci.*, vol. 10, nos. 2–3, pp. 191–203, Jan. 1984.

[106] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, 2000, p. 10.

[107] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.

[108] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Proc. IEEE Proc. Aerosp. Conf.*, Mar. 2002, p. 1125.

[109] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proc. 9th Annu. Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, Sep. 2003, pp. 81–95.

[110] D. Qu, J. Zhang, Z. Hou, M. Wang, and B. Dong, "A trust routing scheme based on identification of non-complete cooperative nodes in mobile peer-to-peer networks," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 22–29. [Online]. Available: https://ieeexplore.ieee.org/document/9343238/

[111] X. Wang, P. Zhang, Y. Du, and M. Qi, "Trust routing protocol based on cloud-based fuzzy Petri net and trust entropy for mobile ad hoc network," *IEEE Access*, vol. 8, pp. 47675–47693, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9022901/

[112] T. Khan, K. Singh, M. H. Hasan, K. Ahmad, G. T. Reddy, S. Mohan, and A. Ahmadian, "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs," *Future Gener. Comput. Syst.*, vol. 125, pp. 921–943, Dec. 2021.

[113] S. S. Desai and M. J. Nene, "Multihop trust evaluation using memory integrity in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4092–4100, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9500235/

[114] A. M. Hilal, A. A. Albraikan, S. Dhahbi, S. S. Alotaibi, R. Alabdan, M. A. Duhayyim, A. Motwakel, and I. Yaseen, "Trust aware oppositional sine cosine based multihop routing protocol for improving survivability of wireless sensor network," *Comput. Netw.*, vol. 213, Aug. 2022, Art. no. 109119.

[115] P. Srividya, L. Nirmala Devi, and A. Nageswar Rao, "A trusted effective approach for forecasting the failure of data link and intrusion in wireless sensor networks," *Theor. Comput. Sci.*, vol. 941, pp. 1–13, Jan. 2023.

[116] T. Khan, K. Singh, M. Manjul, M. N. Ahmad, A. M. Zain, and A. Ahmadian, "A temperature-aware trusted routing scheme for sensor networks: Security approach," *Comput. Electr. Eng.*, vol. 98, Mar. 2022, Art. no. 107735.

[117] Y. Han, H. Hu, and Y. Guo, "Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm," *IEEE Access*, vol. 10, pp. 11538–11550, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9684430/

[118] J. Shahid, Z. Muhammad, Z. Iqbal, A. S. Almadhor, and A. R. Javed, "Cellular automata trust-based energy drainage attack detection and prevention in wireless sensor networks," *Comput. Commun.*, vol. 191, pp. 360–367, Jul. 2022.

[119] Y. Zhao and G. Srivastava, "A wireless mesh opportunistic network routing algorithm based on trust relationships," *IEEE Access*, vol. 10, pp. 4786–4793, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9663156/

[120] J. Jasper, "A secure routing scheme to mitigate attack in wireless adhoc sensor network," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102197.

[121] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, M. Fayaz, and J. Gwak, "Counteracting selfish nodes using reputation based system in mobile ad hoc networks," *Electronics*, vol. 11, no. 2, p. 185, Jan. 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/2/185

[122] G. Sadayan and K. Ramaiah, "Enhanced data security in MANET using trust-based Bayesian statistical model with RSSI by AOMDV," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 8, Apr. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/cpe.5397

[123] V. S. Bhende, A. K. Sinha, and A. A. Junnarkar, "Hybrid-trust model for securing the vehicular ad hoc communications," in *Proc. 2nd Int. Conf. Intell. Technol. (CONIT)*, Jun. 2022, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9848121/

[124] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002, doi: 10.1142/S0218488502001648.

[125] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," Tech. Rep. rfc3561, Jul. 2003. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3561.html

[126] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," Tech. Rep. rfc4728, Feb. 2007. [Online]. Available:https://www.rfc-editor.org/rfc/rfc4728.html

[127] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. Conf. Commun. Architectures, Protocols Appl.*, New York, NY, USA, 1994, pp. 234–244.

[128] R. Bellman, "On a routing problem," *Quart. Appl. Math.*, vol. 16, no. 1, pp. 87–90, 1958.

[129] V. D. Park and M. S. Corson, "A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing," in *Proc. 3rd IEEE Symp. Comput. Commun.*, Jun. 1998, pp. 592–598.

[130] A. Bhattacharyya, "On a measure of divergence between two multinomial populations," *Sankhyā*, vol. 7, no. 4, pp. 401–406, 1946. [Online]. Available: http://www.jstor.org/stable/25047882

[131] J. Han, M. Kamber, and J. Pei, "2—Getting to know your data," in *Data Mining* (The Morgan Kaufmann Series in Data Management Systems), J. Han, M. Kamber, and J. Pei, Eds., 3rd ed. Boston, MA, USA: Morgan Kaufmann, 2012, pp. 39–82.

[132] A. B. S. Yildiz, N. Pholdee, S. Bureerat, A. R. Yildiz, and S. M. Sait, "Sine-cosine optimization algorithm for the conceptual design of automobile components," *Mater. Test.*, vol. 62, no. 7, pp. 744–748, Jul. 2020.

[133] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ, USA: Princeton Univ. Press, Jun. 2020.

[134] H. El Sayed, S. Zeadally, and D. Puthal, "Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks," *Veh. Commun.*, vol. 24, Aug. 2020, Art. no. 100227.

[135] A. Bhargava and S. Verma, "DUEL: Dempster uncertainty-based enhanced—Trust level scheme for VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 15079–15090, Sep. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9767720/

[136] L. Halla-aho, E. Nigussie, and J. Isoaho, "Conceptual design of a trust model for perceptual sensor data of autonomous vehicles," *Proc. Comput. Sci.*, vol. 184, pp. 156–163, Jan. 2021.

[137] S. Misra and T. Ojha, "SecRET: Secure range-based localization with evidence theory for underwater sensor networks," *ACM Trans. Auto. Adapt. Syst.*, vol. 15, no. 1, pp. 1–26, Feb. 2020, doi: 10.1145/3431390.

[138] C. Esposito, O. Tamburis, X. Su, and C. Choi, "Robust decentralised trust management for the Internet of Things by using game theory," *Inf. Process. Manag.*, vol. 57, no. 6, Nov. 2020, Art. no. 102308.

[139] D. Rajavel, A. Chakraborty, and S. Misra, "MobiTrust: Trust-aware pricing scheme for edge-based mobile sensor-cloud for vehicular IoT," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 10033–10043, Sep. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9793647/

[140] M. Simaan and J. B. Cruz, "On the Stackelberg strategy in nonzero-sum games," *J. Optim. Theory Appl.*, vol. 11, no. 5, pp. 533–555, May 1973.

[141] E. Alemneh, S.-M. Senouci, P. Brunet, and T. Tegegne, "A two-way trust management system for fog computing," *Future Gener. Comput. Syst.*, vol. 106, pp. 206–220, May 2020.

[142] L. Wei, Y. Yang, J. Wu, C. Long, and Y.-B. Lin, "A bidirectional trust model for service delegation in social Internet of Things," *Future Internet*, vol. 14, no. 5, p. 135, Apr. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/5/135

[143] J. Al Muhtadi, R. A. Alamri, F. A. Khan, and K. Saleem, "Subjective logic-based trust model for fog computing," *Comput. Commun.*, vol. 178, pp. 221–233, Oct. 2021.

[144] G. H. C. de Oliveira, A. D. S. Batista, M. Nogueira, and A. L. dos Santos, "An access control for IoT based on network community perception and social trust against Sybil attacks," *Int. J. Netw. Manag.*, vol. 32, no. 1, p. e2181, Jan. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/nem.2181

[145] T. Wang, P. Wang, S. Cai, X. Zheng, Y. Ma, W. Jia, and G. Wang, "Mobile edge-enabled trust evaluation for the Internet of Things," *Inf. Fusion*, vol. 75, pp. 90–100, Nov. 2021.

[146] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest—RFTRUST," *Comput. Netw.*, vol. 198, Oct. 2021, Art. no. 108413.

[147] X. Liu, J. Yu, K. Yu, G. Wang, and X. Feng, "Trust secure data aggregation in WSN-based IIoT with single mobile sink," *Ad Hoc Netw.*, vol. 136, Nov. 2022, Art. no. 102956.

[148] A. Jøsang and T. Bhuiyan, "Optimal trust network analysis with subjective logic," in *Proc. 2nd Int. Conf. Emerg. Secur. Inf., Syst. Technol.*, Aug. 2008, pp. 179–184. [Online]. Available: http://ieeexplore.ieee.org/document/4622580/

[149] S. O. Ogundoyin and I. A. Kamil, "A fuzzy-AHP based prioritization of trust criteria in fog computing services," *Appl. Soft Comput.*, vol. 97, Dec. 2020, Art. no. 106789.

[150] F. H. Rahman, T.-W. Au, S. H. S. Newaz, W. S. Suhaili, and G. M. Lee, "Find my trustworthy fogs: A fuzzy-based trust evaluation framework," *Future Gener. Comput. Syst.*, vol. 109, pp. 562–572, Aug. 2020.

[151] S. A. Soleymani, S. Goudarzi, M. H. Anisi, N. Kama, S. A. Ismail, A. Azmi, M. Zareei, and A. Hanan Abdullah, "A trust model using edge nodes and a cuckoo filter for securing VANET under the NLoS condition," *Symmetry*, vol. 12, no. 4, p. 609, Apr. 2020. [Online]. Available: https://www.mdpi.com/2073-8994/12/4/609

[152] V. Krishnaswamy and S. S. Manvi, "Trusted node selection in clusters for underwater wireless acoustic sensor networks using fuzzy logic," *Phys. Commun.*, vol. 47, Aug. 2021, Art. no. 101388.

[153] S. V. Simpson and G. Nagarajan, "A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IoT environment," *Future Gener. Comput. Syst.*, vol. 125, pp. 544–563, Dec. 2021.

[154] B. Pang, Z. Teng, H. Sun, C. Du, M. Li, and W. Zhu, "A malicious node detection strategy based on fuzzy trust model and the ABC algorithm in wireless sensor network," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1613–1617, Aug. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9394421/

[155] A. Almogren, I. Mohiuddin, I. U. Din, H. Almajed, and N. Guizani, "FTM-IoMT: Fuzzy-based trust management for preventing Sybil attacks in Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4485–4497, Mar. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9208705/

[156] H.-J. Zimmermann, *Fuzzy Set Theory-and Its Applications*. Dordrecht, The Netherlands: Springer, 2001.

[157] B. Huber and F. Kandah, "Behavioral model based trust management design for IoT at scale," in *Proc. Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData), IEEE Congr. Cybermatics (Cybermatics)*, Nov. 2020, pp. 9–17. [Online]. Available: https://ieeexplore.ieee.org/document/9291591/

[158] X. Hei, X. Yin, Y. Wang, J. Ren, and L. Zhu, "A trusted feature aggregator federated learning for distributed malicious attack detection," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102033.

[159] D. Wang, Y. Yi, S. Yan, N. Wan, and J. Zhao, "A node trust evaluation method of vehicle-road-cloud collaborative system based on federated learning," *Ad Hoc Netw.*, vol. 138, Jan. 2023, Art. no. 103013.

[160] W. Ma, X. Wang, M. Hu, and Q. Zhou, "Machine learning empowered trust evaluation method for IoT devices," *IEEE Access*, vol. 9, pp. 65066–65077, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9416672/

[161] V. Juneja, S. K. Dinkar, and D. V. Gupta, "An anomalous co-operative trust & PG-DRL based vampire attack detection & routing," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 3, Feb. 2022, doi: 10.1002/cpe.6557.

[162] Z. Tong, F. Ye, J. Mei, B. Liu, and K. Li, "A novel task offloading algorithm based on an integrated trust mechanism in mobile edge computing," *J. Parallel Distrib. Comput.*, vol. 169, pp. 185–198, Nov. 2022.

[163] Y. He, G. Han, J. Jiang, H. Wang, and M. Martínez-García, "A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 3, pp. 811–821, Mar. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9181479/

[164] H. Lin, S. Garg, J. Hu, X. Wang, M. J. Piran, and M. S. Hossain, "Data fusion and transfer learning empowered granular trust evaluation for Internet of Things," *Inf. Fusion*, vol. 78, pp. 149–157, Feb. 2022.

[165] H. N. Bhor and M. Kalla, "TRUST-based features for detecting the intruders in the Internet of Things network using deep learning," *Comput. Intell.*, vol. 38, no. 2, pp. 438–462, Apr. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1111/coin.12473

[166] R. Magdich, H. Jemal, and M. B. Ayed, "A resilient trust management framework towards trust related attacks in the social Internet of Things," *Comput. Commun.*, vol. 191, pp. 92–107, Jul. 2022.

[167] K. A. Awan, I. U. Din, A. Almogren, and J. J. P. C. Rodrigues, "AutoTrust: A privacy-enhanced trust-based intrusion detection approach for Internet of smart things," *Future Gener. Comput. Syst.*, vol. 137, pp. 288–301, Dec. 2022.

[168] M. S. Abdalzaher, M. Elwekeil, T. Wang, and S. Zhang, "A deep autoencoder trust model for mitigating jamming attack in IoT assisted by cognitive radio," *IEEE Syst. J.*, vol. 16, no. 3, pp. 3635–3645, Sep. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9510057/

[169] F. Alqahtani, Z. Al-Makhadmeh, A. Tolba, and O. Said, "TBM: A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications," *Comput. Commun.*, vol. 150, pp. 216–225, Jan. 2020.

[170] H. El-Sayed, H. A. Ignatious, P. Kulkarni, and S. Bouktif, "Machine learning based trust management framework for vehicular networks," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100256.

[171] M. Zineddine, "A novel trust model for fog computing using fuzzy neural networks and weighted weakest link," *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 763–800, Jun. 2020.

[172] S. K. Malchi, S. Kallam, F. Al-Turjman, and R. Patan, "A trust-based fuzzy neural network for smart data fusion in Internet of Things," *Comput. Electr. Eng.*, vol. 89, Jan. 2021, Art. no. 106901.

[173] C. Marche and M. Nitti, "Trust-related attacks and their detection: A trust management model for the social IoT," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 3, pp. 3297–3308, Sep. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9305298/

[174] S. Chinnaswamy and K. Annapurani, "Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks," *Comput. Electr. Eng.*, vol. 91, May 2021, Art. no. 107130.

[175] Y. Trofimova and P. Tvrdík, "Enhancing reactive ad hoc routing protocols with trust," *Future Internet*, vol. 14, no. 1, p. 28, Jan. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/1/28

[176] T. Le and S. Shetty, "Artificial intelligence-aided privacy preserving trustworthy computation and communication in 5G-based IoT networks," *Ad Hoc Netw.*, vol. 126, Mar. 2022, Art. no. 102752.

[177] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019, *arXiv:1901.03407*.

[178] N. Ullah, X. Kong, Z. Ning, A. Tolba, M. Alrashoud, and F. Xia, "Emergency warning messages dissemination in vehicular social networks: A trust based scheme," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100199.

[179] B. Jafarian, N. Yazdani, and M. Sayad Haghighi, "Discrimination-aware trust management for social Internet of Things," *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107254.

[180] A. Alqahtani, H. Kurdi, and M. Abdulghani, "HadithTrust: Trust management approach inspired by Hadith science for peer-to-peer platforms," *Electronics*, vol. 10, no. 12, p. 1442, Jun. 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/12/1442

[181] V. Mohammadi, A. M. Rahmani, A. Darwesh, and A. Sahafi, "Trust-based friend selection algorithm for navigability in social Internet of Things," *Knowl.-Based Syst.*, vol. 232, Nov. 2021, Art. no. 107479.

[182] N. Narang and S. Kar, "A hybrid trust management framework for a multi-service social IoT network," *Comput. Commun.*, vol. 171, pp. 61–79, Apr. 2021.

[183] R. Latif, "ConTrust: A novel context-dependent trust management model in social Internet of Things," *IEEE Access*, vol. 10, pp. 46526–46537, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9762320/

[184] T. Gazdar, O. Alboqomi, and A. Munshi, "A decentralized blockchain-based trust management framework for vehicular ad hoc networks," *Smart Cities*, vol. 5, no. 1, pp. 348–363, Mar. 2022. [Online]. Available: https://www.mdpi.com/2624-6511/5/1/20

[185] M. Cinque, C. Esposito, S. Russo, and O. Tamburis, "Blockchain-empowered decentralised trust management for the Internet of Vehicles security," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106722.

[186] K. Cho and Y. Cho, "HyperLedger fabric-based proactive defense against inside attackers in the WSN with trust mechanism," *Electronics*, vol. 9, no. 10, p. 1659, Oct. 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/10/1659

[187] M. Firdaus and K.-H. Rhee, "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Appl. Sci.*, vol. 11, no. 1, p. 414, Jan. 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/1/414

[188] F. Ghovanlooy Ghajar, J. Salimi Sratakhti, and A. Sikora, "SBTMS: Scalable blockchain trust management system for VANET," *Appl. Sci.*, vol. 11, no. 24, p. 11947, Dec. 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/24/11947

[189] S. Zhang, D. Cao, and Z. Ning, "A decentralized and reliable trust measurement for edge computing enabled Internet of Things," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 24, Nov. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/cpe.7238

[190] H. Liu, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in VANETs," *J. Parallel Distrib. Comput.*, vol. 151, pp. 61–69, May 2021.

[191] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, "Blockchain-based distributed management system for trust in VANET," *Veh. Commun.*, vol. 30, Aug. 2021, Art. no. 100350.

[192] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *J. Parallel Distrib. Comput.*, vol. 152, pp. 144–156, Jun. 2021.

[193] W. Ahmed, W. Di, and D. Mukathe, "Privacy-preserving blockchain-based authentication and trust management in VANETs," *IET Netw.*, vol. 11, pp. 89–111, May 2022, doi: 10.1049/ntw2.12036.

[194] R. Goyat, G. Kumar, M. Alazab, R. Saha, R. Thomas, and M. K. Rai, "A secure localization scheme based on trust assessment for WSNs using blockchain technology," *Future Gener. Comput. Syst.*, vol. 125, pp. 221–231, Dec. 2021.

[195] K. Mershad, O. Cheikhrouhou, and L. Ismail, "Proof of accumulated trust: A new consensus protocol for the security of the IoV," *Veh. Commun.*, vol. 32, Dec. 2021, Art. no. 100392.

[196] K. Wang, C.-M. Chen, Z. Liang, M. M. Hassan, G. M. L. Sarné, L. Fotia, and G. Fortino, "A trusted consensus fusion scheme for decentralized collaborated learning in massive IoT domain," *Inf. Fusion*, vol. 72, pp. 100–109, Aug. 2021.

[197] N. Jiang, F. Bai, L. Huang, Z. An, and T. Shen, "Reputation-driven dynamic node consensus and reliability sharding model in IoT blockchain," *Algorithms*, vol. 15, no. 2, p. 28, Jan. 2022. [Online]. Available: https://www.mdpi.com/1999-4893/15/2/28

[198] R. S. Vairagade and B. Savadatti Hanumantha, "Secure Internet of Things network using light-weighted trust and blockchain-powered PoW framework," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 21, p. e7057, Sep. 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/cpe.7057

[199] Y. Zhao, Y. Wang, P. Wang, and H. Yu, "PBTM: A privacy-preserving announcement protocol with blockchain-based trust management for IoV," *IEEE Syst. J.*, vol. 16, no. 2, pp. 3422–3432, Jun. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9442949/

[200] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2034–2048, Feb. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8926418/

[201] L. Cui, S. Yang, Z. Chen, Y. Pan, Z. Ming, and M. Xu, "A decentralized and trusted edge computing platform for Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3910–3922, May 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8891711/

[202] M. Salimitari, M. Joneidi, and Y. P. Fallah, "BATS: A blockchain-based authentication and trust management system in vehicular networks," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 333–340. [Online]. Available: https://ieeexplore.ieee.org/document/9680563/

[203] A. S. Rocha, B. A. Pinheiro, and V. C. M. Borges, "Secure D2D caching framework inspired on trust management and blockchain for mobile edge caching," *Pervas. Mobile Comput.*, vol. 77, Oct. 2021, Art. no. 101481.

[204] X. Wu and J. Liang, "A blockchain-based trust management method for Internet of Things," *Pervas. Mobile Comput.*, vol. 72, Apr. 2021, Art. no. 101330.

[205] S. K. Arora, G. Kumar, and T.-H. Kim, "Blockchain based trust model using tendermint in vehicular adhoc networks," *Appl. Sci.*, vol. 11, no. 5, p. 1998, Feb. 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/5/1998

[206] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9262037/

[207] F. Li, Z. Guo, C. Zhang, W. Li, and Y. Wang, "ATM: An active-detection trust mechanism for VANETs based on blockchain," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4011–4021, May 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9316986/

[208] D. Kianersi, S. Uppalapati, A. Bansal, and J. Straub, "Evaluation of a reputation management technique for autonomous vehicles," *Future Internet*, vol. 14, no. 2, p. 31, Jan. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/2/31

[209] Y. Wu, J. Liao, P. Nguyen, W. Shi, and Y. Yesha, "Bring trust to edge: Secure and decentralized IoT framework with BFT and permissioned blockchain," in *Proc. IEEE Int. Conf. Edge Comput. Commun. (EDGE)*, Jul. 2022, pp. 104–113. [Online]. Available: https://ieeexplore.ieee.org/document/9860344/

[210] Z. Tu, H. Zhou, K. Li, H. Song, and Y. Yang, "A blockchain-based trust and reputation model with dynamic evaluation mechanism for IoT," *Comput. Netw.*, vol. 218, Dec. 2022, Art. no. 109404.

TERI LENARD is currently pursuing the joint Ph.D. degree in information technology with the University of Geneva, and "George Emil Palade" University of Medicine, Pharmacy, Science and Technology of Târgu Mureş. His research interests include the security protocols in automotive and IoT systems, applications of trusted computing, and trust modeling and management.

ANASTASIJA COLLEN received the Ph.D. degree in information systems from the University of Geneva, in the domain of automated risk assessment. She is currently a Senior Researcher with ISI, University of Geneva. She is also an experienced research and development engineer with a strong knowledge of web oriented and mobile technologies, focusing primarily on the fields of privacy and security. She is a member of the Director Board of InfoSec "continuous education" in information security program and the co-director of the Information Security Group (I-Sec Laboratory). She has contributed to multiple EU-funded projects, including AVENUE, GHOST, and nIoVe. Her current interests include the development of the cyber security solutions and studying human factors on risks perception for IoT devices, smart homes, and smart cities infrastructure.

MERIEM BENYAHYA received the engineering degree from Al Akhawayn University, Ifrane, Morocco. She is currently pursuing the Ph.D. degree with ISI, University of Geneva. She is also a Research Assistant with ISI, University of Geneva. She is also on cybersecurity and data privacy implications and risk assessment tasks on Horizon2020 projects which are focusing on the domain of automated vehicles. Professionally, she successfully managed IT projects from different fields and businesses, including PCI-DSS certifications, data centers infrastructure migrations, change management, IT master plans, and business continuity plans/disaster recovery. She received certification on project management from Temple University, Tokyo, Japan.

NIELS ALEXANDER NIJDAM received the Ph.D. degree in computer science from MIRALab, University of Geneva. His Ph.D. topics included collaborative systems, distributed networking, remote simulations and rendering, and programmable graphics. He is currently a Computer Scientist and a Senior Lecturer ("Maitre d'enseignement et de recherche) with ISI, University of Geneva, and also leading the Information Security Group (I-Sec Laboratory). He worked on several research projects funded by a variety of European and Swiss funding programmes, such as FP6, FP7, H2020, Marie-Curie, AAL, and SNSF and CTI funded projects and has an active role in contributing to and shaping research proposals. He is also coordinating the scientific efforts in H2020 AVENUE, SHOW, and nIoVe projects.

BÉLA GENGE received the B.Sc. degree in computer science from the "Petru Maior" University of Târgu Mureş, Romania, in 2005, and the Ph.D. degree in network security from the Technical University of Cluj-Napoca, Romania, in 2009. He is currently a Marie Curie Alumni and a Professor in computer science with the "George Emil Palade" University of Medicine, Pharmacy, Science and Technology of Târgu Mureş, Romania. He has a three year postdoctoral experience (2010–2013) with the Joint Research Centre of the European Commission, Institute for the Protection and Security of the Citizen, Italy. He has authored several papers in the *International Journal of Critical Infrastructure Protection*, IEEE TRANSACTIONS ON SMART GRID, IEEE SYSTEMS JOURNAL, *Communications of the ACM*, and IEEE/IFIP Networking. His research interests include security and resilience of industrial cyber-physical systems, ensemble anomaly detection, and network security in general. He received best paper awards at IEEE INDIN 2015 and IEEE INDIN 2017.