IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 19, 2021, accepted May 27, 2021, date of publication June 4, 2021, date of current version June 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3086534

ETAS: An Efficient Trust Assessment Scheme for BANs

ANAND KUMAR[1], KARAN SINGH[1], (Senior Member, IEEE), TAYYAB KHAN[1], ALI AHMADIAN[2], MOHAMAD HANIF MD. SAAD[2], AND MANISHA MANJUL[3]

[1]School of Computer and Systems Sciences, JNU, New Delhi 110067, India
[2]Institute of IR 4.0, The National University of Malaysia, Bangi 43600, Malaysia
[3]CSE, G.B. Pant Government Engineering College, New Delhi 110020, India

Corresponding author: Karan Singh (karan@mail.jnu.ac.in)

This work was supported by Universiti Kebangsaan Malaysia through the Prime Impact Fund (DIP) Grant under Grant DIP-2020-021.

ABSTRACT A wireless body area network (WBAN) is a wireless network of wearable computing devices and intelligent physiological sensors. The intelligent physiological sensors collect and process sensitive data from the patient body. The security, reliability, and trustworthiness of sensitive data collected and processed by intelligent physiological sensors are critical due to its unique application domain. Moreover, consistent and reliable data gathering along with its transmission also plays a vital role in WBANs. Trust management (in BANs) has been found as a useful tool to improve cooperation among sensor nodes, security as well as reliability. The paper recommends a novel and efficient, lightweight trust assessment scheme (ETAS) suitable for health application domains and does not rely purely on any encryption technique. The primary purpose is to develop an exciting comprehensive, novel trust estimation framework for BANs to enhance reliability, dependability, security by isolating compromised (hotspot) nodes with great resource efficiency. ETAS incorporates several exclusive (unique) features like efficient trust evaluator, secure and attack resistant, along with competent trust aggregator function to achieve comprehensive trust score. The trust evaluator function is a multi-trust (communication trust, data trust, and energy trust) strategy to deal with severe internal security threats such as badmouthing attack, ballot-stuffing attack, sybil attack, traitor attack, etc. with less resource consumption. Moreover, ETAS incorporates both the success rate and misbehavior component during trust evaluation. The success rate record the number of successful/unsuccessful interactions among sensor nodes in terms of packet send/receive. The misbehavior component keeps records of current and past misbehavior of sensor nodes for effective decision making. Moreover, ETAS focus on the frequency of interaction among biomedical sensor nodes within a specified period to analyze their behavior for efficient trust decisions. Furthermore, ETAS incorporates temperature, data trust as well as the trust score of biomedical sensors to identify hotspot nodes in BSN. ETAS offers full flexibility to adjust the trust threshold, trust domain, reward, and punishment term according to system and application requirements. ETAS's efficiency is validated through several outcomes (MATLAB R2019a) along with theoretical analysis in terms of energy consumption, attack detection, mitigation, trust computation cost, and packet delivery ratio.

INDEX TERMS Trust assessment, body area network (BAN), security, trust, recommendation.

I. INTRODUCTION

A wireless body area network (also known as WBAN, BAN, BSN, and MBAN used interchangeably) is a multi-hop, temporary wireless network of low powered BAN devices, e.g., Electrocardiogram (ECG), Electromyography (EMG), Electroencephalogram (EEG)) that maybe, implants, mounted on/inside the body in a fixed position [1]. A WBAN system is a consequence of wireless sensor network that employs WPAN as gateways devices to attain longer ranges as well as adequate access to patient real-time health records through internet service [2]. WBANs have recently emerged and suggested vital requirements for various telehealth applications such as blood pressure monitoring and sugar level monitoring without dependence on any fixed (static) infrastructure such as hospitals. A WBAN consist of inexpensive, limited

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

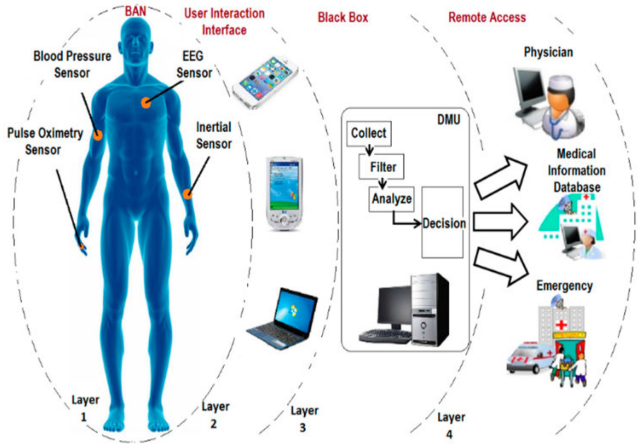

FIGURE 1. WBAN architecture and application scenario [5].

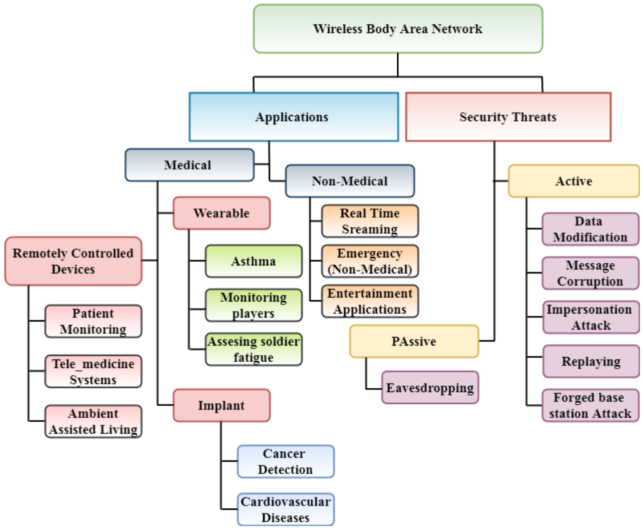

FIGURE 2. WBAN applications and security threats.

power intelligent physiological sensors (IPS). IPSs monitors, accumulate and process the critical data from the patient body. IPSs employ multi-hop communication to monitor health conditions (domains) as well as early detection of various health status or physiological changes in patients affliction from several chronic diseases such as heart attacks, asthma, diabetes without requiring any location information through measuring changes [3]. Although if the location of the patient is required, then motion detector sensors help to discover patient's locations. The monitored (recorded) medical information is processed by an external processing unit and instantly transmitted to worldwide doctors. Moreover, emergency alarms (message) can be sent through a computer/mobile system to save the life of patients whenever any emergency such as heart attack, insulin level declines, etc. is detected. If insulin level declines, the sufficient dose is wirelessly injected by doctors with the help of data terminals [4].

The IEEE 802.15.6 is the most modern standard to facilitate security in WBANs. WBANs entirely rely on the recorded (monitored) information via IPSs (or biosensors) as any incorrect information about health might be dangerous for patients' life [5]. In such cases, when the sensor node (SN) itself behaves maliciously (intentionally or unintentionally due to primitive stage technology issues etc.), cryptographic (authentication, authorization, hash) techniques [6]–[8] are infeasible to protect the network since they impose high overhead as well as unable to mitigate insider attacks [8]–[10]. Fig.2. shows various applications and security threats in WBANs.

A. TRUST AND REPUTATION SYSTEMS

Trust management schemes (TMSs) are proved as an efficient and reliable tool [17], [18] to catch as well as mitigate (diminish) malicious IPSs. Trust evaluation monitors the IPSs behavior, estimates the trust value, and then quantified it into highly trusted, trusted, and distrusted [19], [20]. Trust value (score) is a level (quantification or measure) of belief of one entity towards another entity [21], [22]. The concept of trust is originated from human society and hence plays an essential role in our everyday lives. Trust is defined as a relationship between trustor and trustee. Trust describes a subjective relation among entities, while reputation is an opinion about an entity [24], [25]. These opinions are provided by participating entities in a relationship. Hence trust may be used to determine the reputation of an entity, and reputation is used to determine the trustworthiness of an entity [31]. Trust specifies the reliability or trustworthiness of an entity [32]. Trust is a belief [45] that ensures the entity as secure and reliable. Trust plays an essential role in improving reliability as well as cooperation among sensing devices. Trust has great significance and influence on the quality and integrity in healthcare applications since it guarantees a correct and timely diagnosis of the patient. The objective of trust systems is to evaluate the probability expectation that a given event occurred. In the case of sensor data, this event would be that the sensor data really reflects the actual physical environment [48], [49]. Reputation systems have been developed in order to identify compromised nodes based on their behavior. Reputation is based on a collection of evidence of good and bad behavior is undertaken by other entities [50].

Fig.3. shows various possible solutions to achieve security from internal/external attacks. Trust is dynamic, context-dependent as well as complex concept in WSNs. There are various advantages [51]–[53] of trust management schemes (trust models) such as

- Detect various kinds (intentional or unintentional) of misbehaviors of IPSs.
- Provide access control as well as reliable shorter routing paths
- Monitor and detects delay contributing IPSs, estimate trustworthiness level of communicating parties in real-time healthcare applications.

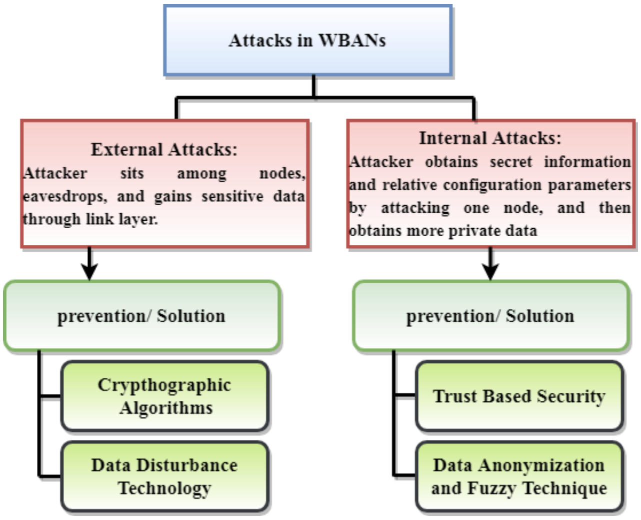
Attacks in WBANs
External Attacks:
Attacker sits among nodes, eavesdrops, and gains sensitive data through link layer.
Internal Attacks:
Attacker obtains secret information and relative configuration parameters by attacking one node, and then obtains more private data
prevention/ Solution
prevention/ Solution
Crypthographic Algorithms
Data Disturbance Technology
Trust Based Security
Data Anonymization and Fuzzy Technique

FIGURE 3. WBAN attacks and their prevention techniques.

- Impose lower overhead (resource, computation) than cryptographic algorithms.
- Vital for internal threats (badmouthing attack, ballot-stuffing attack, whitewashing attack, Sybil attack, traitor attack, grudge attack, etc.) and ensure data integrity as well as data freshness by the continuous monitoring process.
- Appropriate to provide security for the energy-starved environment with low computational and communication costs.

Fig.3. shows various possible solutions to achieve security from internal/external attacks. Trust is dynamic, context-dependent as well as complex concept in WSNs.

Fig. 4 summarizes the motivation for trust in WBSN, their design criteria, types as well as associated attacks in a well-structured way.

The reliability of WBANs depends on the cooperation (collaboration) level of nodes as well as data generated by them [26]. Sometimes it is challenging to know about interactions of nodes within the specified time. Moreover, interacting nodes are trustworthy or not is itself a big deal [27], [28]. To resolve the aforementioned issues, we have designed anefficient trust assessmentscheme (ETAS) that incorporates triple trust (energy trust, communication trust, and data trust) to deal with selfish nodes and malicious (unexpected) behavior. Communication trust is a level of assurance that nodes are communicating or not in a specified time or not. Depending upon the number of interactions, we evaluate communication trust. Data trust is a level of assurance of data collected, generated, and exchanged by physiological sensors is trustworthy or not. The concept of energy trust helps to resolve the situation when a node might misbehave due to a faulty (insufficient) battery. Section III discusses the Threat (adversarial) Model, which takes into account the adversaries' types and their power, in addition to the possible threats that are performed by those adversaries. ETAS incorporate three types of biosensor nodes, namely the IPS, the relay nodes and the sink nodes along the details of the trust based security scheme.

B. MOTIVATION

Body sensor networks (BSNs) consist of various IPSs to monitor patient health status remotely. The quality of data generated and collected through sensors (i.e. data freshness without any delay) plays a vital role in decision-making for better care of the patient. There are several issues and challenges such as security [1]–[5], data quality [5] and its management [6], sensor validation [7], data consistency and freshness [8]–[10], interoperability [11], [12], cost [13], transmission delay, consistent performance [14], [15] and inference [16]. There exist [2], [4], [7]–[10], [17], [20], [24]–[26], [28], [29], [32], [33], [35]–[40], [42], [43], [45], [47] various secure models for WBANs based on authentication, authorization, access control [11], key management [10], [36], [51], and encryption but these existing models are unable to satisfy the fundamental requirement (real-time response, resource efficiency, dependability, data availability, and integrity) of body sensor networks (BSNs) since they impose extra overhead by employing heavyweight algorithmsas well as not employ multi-trust concept. Moreover, cryptographic security solutions are not effective in alleviating internal adversaries such as badmouthing attack,sybil attack, traitor attack, grudge attack, ballot-stuffing attack, On-off attack, etc. Since they assume that all the participated entities are trusted (reliable), so provide protection against only external attacks. Existing WBANs trust models [2]–[7], [9], [10], [34], [35], [42], [43] failed in terms of dependability, fast response and resource efficiency due to the incorporation of week trust function (linear, static). [17], [23], [43], [44] states that static trust functions with stable punishment coefficient are vulnerable to security threats. Furthermore, aforementioned trust schemes do not consider temperature of biomedical sensors nodes since increased temperature can damage sensitive tissues. Due to the unreliable communication medium, the transmitted information (data set) of sensors readings must be validated to diminish possible weaknesses as well as false alarms generations. The patient health data observed by the sensor nodes must be secure, has limited access, and should not mix with other patient data during collection as well as transmission. Moreover, an efficient security model for resource-constrained WBANs should be accurate, cost-effective, real-time responsive, scalable, transparent, and less complex since BANs deals with sensitive and significant health data [45]–[52].

The paper provides a motivation and scope for the researchers in the field of trust based security of BANs. Let us discuss a motivating example for researchers and scientist. For example, "if the blood glucose sensor of a diabetic patient is hacked, and a faked high blood glucose concentration value is reported, the insulin pump will be activated, and a dose of insulin is injected, which can lead to various chronic diseases or even more severe result if the injection of insulin occurs too frequently. Therefore, in addition to the existing security

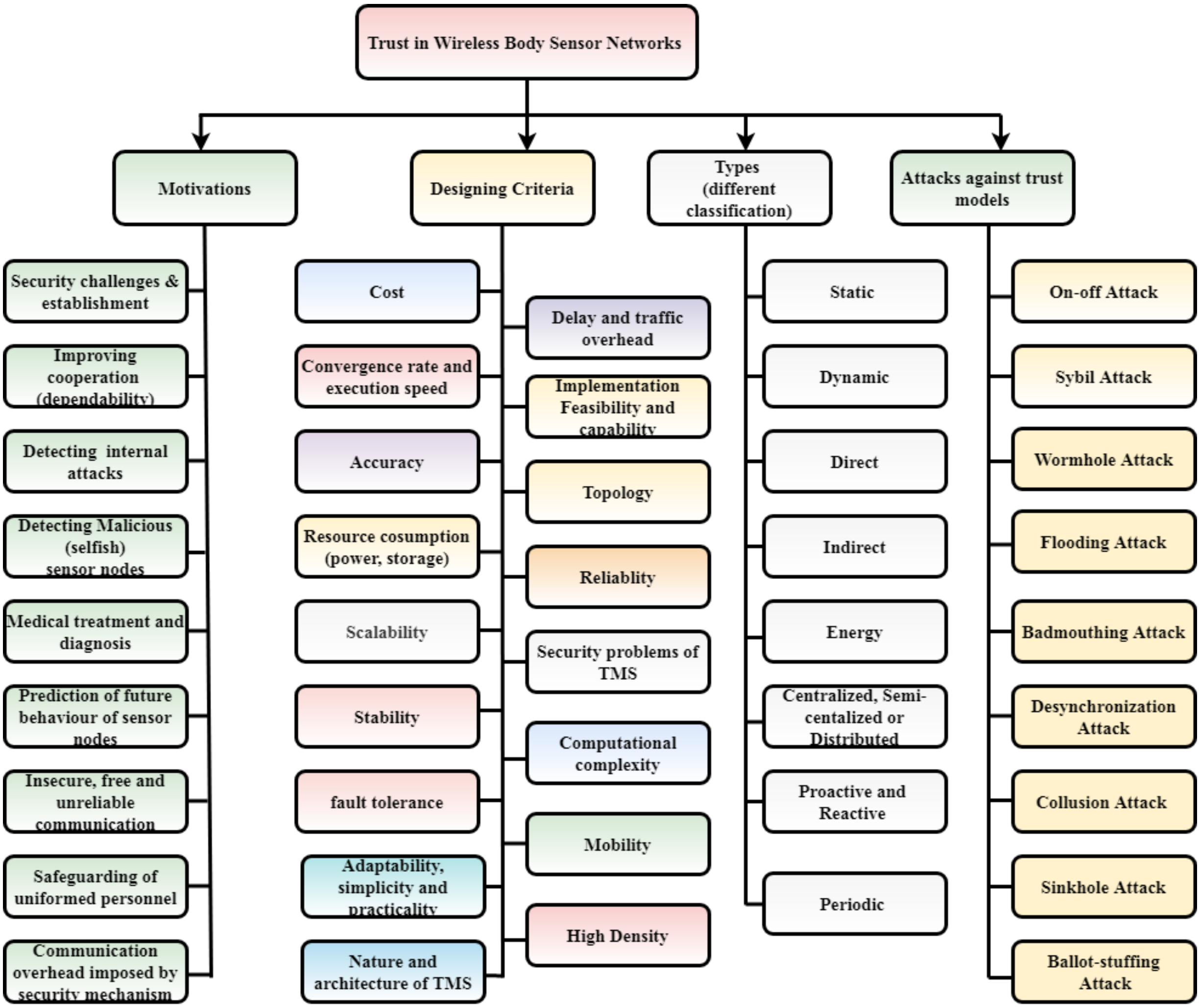
Trust in Wireless Body Sensor Networks
Motivations
Designing Criteria
Types (different classification)
Attacks against trust models
Security challenges & establishment
Improving cooperation (dependability)
Detecting internal attacks
Detecting Malicious (selfish) sensor nodes
Medical treatment and diagnosis
Prediction of future behaviour of sensor nodes
Insecure, free and unreliable communication
Safeguarding of uniformed personnel
Communication overhead imposed by security mechanism
Cost
Delay and traffic overhead
Convergence rate and execution speed
Implementation Feasibility and capability
Accuracy
Topology
Resource cosumption (power, storage)
Reliablity
Scalability
Security problems of TMS
Stability
Computational complexity
fault tolerance
Mobility
Adaptability, simplicity and practicality
High Density
Nature and architecture of TMS
Static
Dynamic
Direct
Indirect
Energy
Centralized, Semi-centalized or Distributed
Proactive and Reactive
Periodic
On-off Attack
Sybil Attack
Wormhole Attack
Flooding Attack
Badmouthing Attack
Desynchronization Attack
Collusion Attack
Sinkhole Attack
Ballot-stuffing Attack

FIGURE 4. Trust in WBANs: Motivation, design criteria, types and attacks.

solutions for BANs, it is also critical to evaluate the trust in" BANs. Moreover, sometimes fresh (current monitored) data is not accessible to doctors that might lead to non-detection of various severe abnormalities, which in turn leads to serious consequences (i.e., death) on the patient.

C. OUR CONTRIBUTION

To eradicate the drawbacks of existing inadequate trust models [1], [3], [5]–[8], [10], [15], [17], [27], [32], [34], [39], [40]–[50] and other security schemes [2], [4], [9], [10], [20], [24]–[26], [28], [29], [35]–[39], [42], [43], we have designed a comprehensive and innovative trust model incorporating several unique (distinctive) features to enhance collaboration and dependability among IPSs for developing a robust and trusted BSN system. These unique features are listed below as follows

1) Generate and assign a unique identity (ID) to every IPSs for more natural and secure communication as well as to achieve protection from external threats.
2) present a vigorous distributed trust model by incorporating a multi-factor (temperature, misbehavior component, data trust, energy trust, number of interactions) trust approach to ameliorate collaboration and dependability among IPSs with moderate communication overhead. Moreover, our proposed scheme ETAS provides better telehealth service by considering the temperature factor of IPSs since high temperature of biomedical sensor nodes generated due to excessive communication can damage sensitive tissues.
3) ETAS provide a flexible (adjustable) reward and penalty coefficient in the trust model. These parameters can be tuned according to a patient's health condition (i.e., application requirements). Proposed approach allows only trusted nodes to be part of BSN by isolating hotspot nodes. ETAS is independent of the platform and specific routing scheme.

In précis, our research work is considerable and dissimilar from previous existing work that incorporates temperature

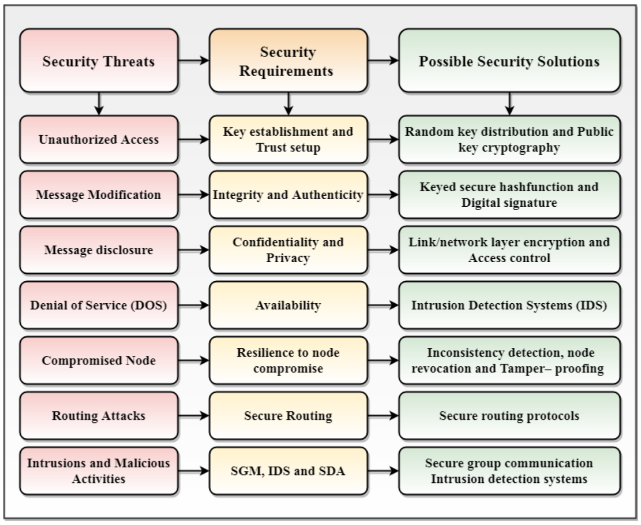
Security Threats
Security Requirements
Possible Security Solutions
Unauthorized Access
Key establishment and Trust setup
Random key distribution and Public key cryptography
Message Modification
Integrity and Authenticity
Keyed secure hashfunction and Digital signature
Message disclosure
Confidentiality and Privacy
Link/network layer encryption and Access control
Denial of Service (DOS)
Availability
Intrusion Detection Systems (IDS)
Compromised Node
Resilience to node compromise
Inconsistency detection, node revocation and Tamper– proofing
Routing Attacks
Secure Routing
Secure routing protocols
Intrusions and Malicious Activities
SGM, IDS and SDA
Secure group communication Intrusion detection systems

FIGURE 5. WBAN: Security threats, requirements and possible security solutions.

unaware static trust functions without dynamic compensation. Our trust assessment scheme secures the WBANs by considering cooperative interactions and non-cooperative interactions during trust evaluation. To the best of our knowledge, ETAS is the first trust assessment model that focuses on frequency of interactions to decide the right track for accurate trust evaluation. ETAS incorporate temperature, misbehavior of IPSs with communication trust and data trust to improve the effectiveness of trust model. The effectiveness, efficiency, and affirmation of the ETAS are demonstrated by simulation (MATLAB R2019a) experiments as well as theoretical analysis. The leftover part of this manuscript is prepared into five more sections. Section II focuses onsome recent proposals for WBANs security with their limitations and comparative analysis. Section III and IV discuss the suggested trust modelas well as project their ample validation, respectively. Section V shows the simulation analysis and reveals the achievements of the projected scheme (ETAS), and finally, Section VI concludes the entire research work and provide future direction.

II. RELATED WORK

This section discusses the literature review of existing secure models in BANs. However, considerable research work has been carried out to protect BSNs; only the nominal effort is made for internal adversaries [29], [30] such as badmouthing attack, ballot-stuffing attack, whitewashing attack, On-off attack [1], etc. by employing the trust concept that can lead to extremely unsafe health conditions. We have rigorously studied various research articles [1], [3], [5], [6]–[16], [30]–[50] related to authentication and trust in a body sensor network with their strength as well as research gaps and observe security threats along with their requirements and possible prevention techniques (refer figure 5).

Li *et al.* [10] recommend a user-aided ''multi-party authenticated key agreement protocol'' known as group device pairing (GDP) to establish initial trust. The initial trust among SNs is set up by generating multiple shared secret keys. GDP employs a symmetric-key cryptography scheme to perk up the performance of the authentication method. Moreover, GDP does not rely on any supplementary hardware appliance. In this paper, Key management and initial trust establishment in WBANs are two main issues are addressed with the help of device pairing. The author states that it is challenging as well as demanding tasks to provide a user-friendly and efficient trust initialization process in a resource constraint WBAN. Moreover, the author believes that key pre-distribution based security solutions are not suitable for BANs.

Mana *et al.* [32] suggest a trusted based key management scheme for WBANs to enhance the protection and confidentiality of sensitive health data by managing the symmetric session keys.. With the proposed scheme, secure data transmission can be achieved by proficiently generating and distributing cryptographic keys among base station (sink) and sensor devices. Theoretical analysis exhibits its effectiveness in terms of energy-saving and security.

Liu *et al.* [33] projected a ''Certificateless Remote Anonymous Authentication'' method for WBANs which is a lightweight and efficient system to guard the privacy of BSN users. With this certificate less signature (CLS) scheme, Patents can get the benefit of remote medical health services in an efficient and secure way. The CLS scheme as the cryptographic primitive, which is cost-effective, efficient and provably secure against existential forgery on adaptively chosen message attack in the random oracle model. the protocols use an anonymous account index instead of a WBAN client's real identity to access WBAN service, thereby preventing the potential privacy leakage to application providers (AP) and network managers (NM).

Li *et al.* [34] discussed a trust management scheme (TMS) to deal with the security issues in BANs. The author employs the recommendation trust of WBAN node's and conducts several experiments to analyze the usefulness and validity of the projected scheme. The authors state that the data generated from the WBAN is essential and highly sensitive, so trust evaluation is essential to discover the faulty SNs as well as enhance dependability. Recommendations trust values of all neighbor of each node is stored in matrices, and their similarly is measured using a cosine product vector rule by identifying the angles between them. A collaborative filtering approach and Resnick's standard prediction formula is employed to compute the trust score of BAN nodes. Top k nodes are selected as trusted neighbors and used in Predicted trust calculation. The effectiveness of BAN-Trust scheme is evaluated using precision and recall on GloMoSim 2.03 with simple weighted voting method. There are various research gaps in this paper such as i) not comprehensive ii) no severity analysis, iii) no mathematical proof regarding the robustness of trust model iv) various attacks are not considered.

Guo *et al.* [35] proposed a ''A Lightweight Encryption Scheme Combined with Trust Management for Privacy-Preserving in Body Sensor Networks''. The lightweight encryption scheme incorporated with trust management is based on mix a cipher algorithm which is used to improve the privacy and reliability of sensitive health information. Moreover, authentication scheme with trust management helps to find the reliable nodes that can participate in processing and transmission of private data. In The major limitation of this scheme is that various attacks are not considered during simulation. Moreover, there is no theoretical analysis for its validity as well as complexity with existing schemes also not discussed in comprehensive way.

Hayajneh *et al.* [36] designed a lightweight authentication protocol for Medical Sensor Networks to spot various security and privacy issues during remote patient health condition monitoring. The proposed protocol for BSNs is a modified Rabin authentication algorithm with the Jacobi that is a public key-based authentication based protocol in which SNs gather health information and performs appropriate action as per the received command. The key plan of the suggested authentication protocol is to enhance the "signature-signing process" that makes it appropriate for delay-sensitive medical sensor network applications. The research outcomes shows good efficiency in terms of providing authenticated commands to the SNs embedded (mounted) on/inside the body. The performance and efficiency are measured using the MIRACL library, Field Programmable Gate Array (FPGA) and Tmote Sky mote with different hardware settings, respectively.

Omala *et al.* [38] recommended a well-organized remote authentication scheme (RAS) for WBANs. The author states that physiological data of a patient in limited range WBANs is forwarded to the remote server via intermediate portable devices (Smartphone) might be captured and modified by internal/external adversaries. The modified physiological data due to an open environment might lead to a poor diagnosis, which may be lethal for a patient. In order to resolve the aforementioned issues and to improve security, reliability as well as privacy, we have designed a robust RAS for WBANs in terms of attacks mitigation, convergence as well as performance. The proposed schemes reduce 50% of running time at the client side when compared to other protocols.

Bhangwar *et al.* [39] suggest a "Trust and Thermal Aware Routing Protocol (TTRP)" for WBANs to improve reliability, confidentiality, the privacy of transmitted physiological data. The authors state that conventional cryptographic, as well as biometric algorithms are not beneficial in BSNs since they do not deal with malicious behavior of nodes, cost-inefficient as well as impose high complexity than trust-based schemes. Moreover, the temperature generated by sensor nodes due to electromagnetic radiations might be dangerous for sensitive tissues. To resolve the aforementioned issues and limitations of existing security schemes for WBANs, we proposed a resource-efficient, lightweight, temperature and trust-based thermal aware solution for WBANs. TTRP is a multi-factor routing scheme that incorporates trust as well as the temperature of nodes to detect (restrict) and segregate faulty nodes in order to provide a reliable healthcare service.

Priya *et al.* [40] discussed a trusted routing scheme for WBANs to diminish the information misfortune. The authors assume that sensor devices are implanted on the human body in a clustered way where cluster head (CH) is elected using well known "particle swarm optimization" (PSO) and accumulate the trust scores of other SNs. We apply a fluffy (fuzzy) based trust induction model along with scheduling algorithms as well as self-adaptive greedy buffer allocation to reduce energy consumption. Moreover, the proposed secure model improves the delivery ratio as well throughput, reduce congestion in comparison to other existing schemes. A trust routing path is selected by considering the trusted sensor nodes.

Chitra *et al.* [41] proposed a "Fault aware trust determination (FATD) algorithm for wireless body sensor network (WBSN)". The trust algorithm assigns trust score between −1 to 1. The trust score of the biomedical sensor node is computed by incorporating node's movement, receiver signal strength as well as battery terminal voltage. The proposed work is simulated on MATLAB to analyze the efficiency and throughput. The major drawback of this work is that FATD is not robust against BAN's attack since they don't incorporate adequate trust metrics for achieving security.

Anguraj *et al.* [42] projected a "Trust-based intrusion detection and clustering approach for wireless body area networks" for efficient transmission of critical medical data in an open environment. The cluster head within a group is elected by employing a multi-objective firefly algorithm. Hybrid encryption method and target functions are used to encrypt sensitive data and improve throughput, respectively. The simulation results carried out using NS-2 exhibit acceptable performance in terms of packet delivery ratio (PDR), delay, precision, and recall.

Roy *et al.* [43] proposed "A Novel Trust Evaluation Model Based on Data Freshness in WBAN" to detect selfish (non-eligible) nodes by employing a trust model along with data freshness factor. The author states that health-related data is sensitive and prone to various threats that can be efficiently protected by lightweight trust models instead of cryptographic algorithms. A selfish node performs unexpected in several ways, such as dropping the fresh data packet and forward old (or useless) data to destination for incorrect decision-making. Moreover, sometimes-unintentional problems are raised due to the low residual energy of IPS or network issues such as congestion, delay, etc.

Wang *et al.* [44] discussed a trust improvement technique based on trusted platform module(TPM) for clustered WSNs by dividing the network into numerous rounds. Every round employs a "setup phase" as well as a "steady-state phase." The proposed method employs Setup μTESLA, STEADY-μTESLA, SET-SCHNORR authentication protocols to make it lightweight, energy-efficient, attack-resistant along with less communication overhead. The key role of the TPM is to assess the integrity of cluster heads (CHs) and to establish as well as maintaining trust relationships among SNs as CHs play a vital role in node misbehavior (attack) detection.

However, no valid proof is given to justify its suitability in real-time industrial applications.

Ostad-Sharif *et al.* [45] recommended a key agreement protocol for WBANs to provide security and reliability. To prevent the WBANs from the internal attacks, privacy protection and mutual authentication schemes are required to protect the critical and confidential physiological data of a patient. To fulfill the aforementioned purpose, we design a robust authentication and key agreement protocol that incurs less communication overhead as well as mitigate de-synchronization attack and wrong session key agreement attack. Moreover, the AVISPA tool and a random oracle model are employed to comparatively examine the security level of the proposed scheme. The suggested scheme is also robust against active as well as passive attacks.

Nidhya *et al.* [46] discussed a survey related to security as well as privacy issues of sensed heterogeneous (critical) sensed data in remote healthcare systems using WBANs. The author states that critical health data plays a vital role in accurate decision-making that should be accessed by certified medical professionals for any action required for better treatment. The author [32], [33], [37] discusses the advantages and limitations (security threats levels) in WBANs. These security threats can emerge either data (information) gathering level, storage level, or transmission level. The security threats at data collection levels are data collision attack, jamming attack, selective forwarding attack, sybil attack, data flooding attack, and spoofing attack. Moreover, the security threats at transmission-level are defined as eavesdropping, data tampering attack, man in the middle attacks, scrambling attacks, signaling attacks, data interception attack, hello flood attack, and wormhole attack. The security threats at storage levels are malware attack and social engineering attacks etc. the author states that access control, availability, dependability, and flexibility are major privacy requirements in WBANs.

Karchowdhury *et al.* [47] present an exhaustive survey on attacks for WBANs. The authors explained the reasons for the vulnerability of security threats arise due to its Adhoc, openness topology and suggest various prevention as well as privacy techniques to improve the efficiency of remove health-care systems. Moreover, authors state that remote healthcare through WBANs is a demanding as well as an attractive application area of WSNs because of its benefits on humans life. With remote health care using WBANs, a patient suffering from diabetes, sugar, blood pressure, Nosocomephobia, and hypertension need not admit (stay) in hospitals for many days as well as he can do their normal activities. The author suggests that a robust security scheme is vital to protect sensitive data from several internal/external threats and discuss layer-wise attacks with their definitions and misbehavior.

Usman *et al.* [48] propose a "trust-Based DoS Mitigation Technique for Medical Implants in Wireless Body Area Networks" by employing a three-level trust model as well as considering the resource limitation of sensor devices. We allowed the maximum data rate at each level according to the environment (home, office, public place) to transmit sensitive information. Moreover, the non-sharable trust threshold is changed by the base station according to environmental conditions. With this three-level trust model, along with a non-sharable trust threshold, these schemes effectively detect and isolate DoS attack. Although, no mathematical, as well as theoretical analysis, are given in favor of its robustness.

Remu *et al.* [49] proposed a "Naive Bayes based Trust Management Model for Wireless Body Area Networks" to ensure security from selfish nodes. The authors have employed a naïve based classifier to classify a biomedical sensor node as a trusted or faulty node. The proposed model has been trained in MATLAB by taking 80 data sets randomly and got predicted classification as HIGH (H), LOW (L) and MOD-ERATE (M). The major limitations of this scheme are uncertainty of trust estimation and computational complexity. Moreover, trust update mechanism is not defined.

Roy *et al.* [50] presented a "Security and Privacy Issues in Wireless Sensor and Body Area Networks." The authors focus on the importance of body area networks in monitoring the vital physiological parameters of a patient.

Moreover, the authors discuss the security issues and provide motivation to design efficient lightweight security schemes. Furthermore, the paper discusses the threats as well as countermeasures and lists some existing papers with their research gaps.

Jiang *et al.* [56] suggested a "Trust based energy efficient data collection with unmanned aerial vehicle (TEEDC-UAV) in edge network" to improve network lifetime. TEEDC-UAV scheme employs an ant colony based unmanned aerial vehicle (UAV) trajectory optimizationalgorithm to balance energy consumption. UAV trajectory optimization reduces the cost and time of data collection. Moreover, trust concept is used to identify reliable sensor nodes for the collection of qualitative data and to ensure network security. Although, experimental results proves it efficiency but the suggested scheme is complex and the trust model is not clearly defined. Moreover, punishment and reward to faulty nodes is not discussed under trust evaluation.

Li *et al.* [57] proposed a "Trust data collections via vehicles joint with unmanned aerial vehicles in the smart Internet of Things (T-SIoTs)" to achieve acceptable security and energy efficiency at the same time. Very first, data center finds trusted mobile data collector using historical datasets. Static data collectors are established to secure coverage regions of data collections. Vehicular collectors can only communicate data to either trust-based mobile stations or static sensor stations, instead of sending data to other unreliable vehicles. Second, UAVs arranged by the data center will accumulate data stored in both static and mobile sensor stations then transmit data to the data center. In the T-SIoTs scheme, UAV's trajectoriesare designed according to shortest-distance-first routing scheme. Comparative theoretical analysis and experimental results show that the T-SIoTs design can attain better performances on aspect of security and aspect of energy consumptions.

Mehmood *et al.* [58] proposed "A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in WBANs" to ensure the reliability and privacy by employing trust and cryptography mechanism respectively. Trust-Based ERCS incorporate simple static trust function with fuzzy logic EDAS-based ranking. Although, authors' claims its efficiency in terms of reliability, service delivery ratio, reduced average delay but static trust function is inefficient to detect insider adversaries and cryptography mechanism impose high communication overhead. Moreover, weight assignment approach is not clearly specified during trust aggregation.

Huang *et al.* [59] suggested a "BD-VTE: a novel baseline data based verifiable trust evaluation (VTE) scheme for smart network systems" to guarantee security at a reasonable cost. BD-VTE scheme includes VTE system, Effectiveness-based Incentive (EI) mechanism, and Secondary Path Planning (SPP) strategy, which are respectively used for reliable trust evaluation, reasonable reward, and efficient path adjustment. Moreover, the suggested scheme improve accuracy and data collection rate. Mobile vehicles are used for data collection and an unmanned aerial vehicle provides reliable safety assurance for mobile vehicles. The limitations of this research are as follows i) limited mobile vehicles on the infrastructure-less environment ii) high computational overhead iii) real-time implementation is difficult.

Ramaswamy *et al.* [60] proposed a "Social and QoS based weighted trust model for secure clustering for WBANs" to improve network lifetime by minimizing energy consumption and reducing dead nodes. The suggested social-and QoS-based trust scheme identify malicious nodes and avoid internal soft attacks during communication. It provides comprehensive survey Table for various safe and vulnerable trust based protocols for clustering in terms of trust computation, QoS, energy consumption and application of the network. Trust value (T) is computed using subjective Logic process as a triplet $\{b, d, u\}$ where b, d *and* u represent belief, disbelief and uncertain respectively with the property $b + d + u = 1$. The node trust value is computed using $\frac{2b+u}{2}$ where $\text{b} = \frac{s}{s+f+1}$ and $u = \frac{1}{s+f+1}$. Comparative results at varying malicious node percentage withLEACH and LEACH-MM exhibit acceptable performance in terms of minimum energy consumption, packetforwarding, minimum packet drop,and successful packet delivering. Moreover it is shown that the suggested scheme prevents from selective forwarding attack, Sybil attack, and HELLO Flooding attacks.

Ilyas *et al.* [8] proposed an efficient "Trust-based energy-efficient routing protocol for Internet of things–based sensor networks" to improve network throughput, enhance security by isolating malicious nodes, minimize packet latency and prolong network lifetime. The suggested security scheme is energy harvesting based three-layer clustered WSN routing protocol to encounter faulty nodes from next successive rounds. Moreover, sink node elect the CHs depending on the cost function (CF) value and routing efficiency is improved by checking the link effectiveness by employing hardware-based link quality estimators. CF value is computed using <Link qualities, residual energies, distance to sink node, total energies>. NS-3 simulator is used to compare and validate the research work.

TABLE 1. Attacks addressed based on the monitored behavior [6], [8].

Trust metric	Monitored behavior	Attack addressed
Data packets forwarded	Data packet (message) forwarding	Selfish behavior,Black-hole, denial of service, sinkhole, selective forwarding,
Stability of reported values/data	reliability of sensing results, reported values such as energy, humidity	Compromised nodes
Reputation	Trust value observed by third parties	Badmouthing attack
Battery/lifetime	Remaining power resources	Node availability
Cryptography	Capability to perform encryption	Authentication attacks
Sensing communication	Reporting of events (application-specific)	Selfish node behavior at the application level
Packet address modified	Address of forwarded packets	Sybil, wormhole
Control packets forwarded	Control message forwarding	Control/routing message dropping
Availability based on beacon/hello messages	Timely broadcast of periodic routing information	Passive eavesdropping, selfish node
Routing protocol execution	Routing protocol-specific actions	Misbehaviors associated to particular routing protocol actions
Data packet precision	Data integrity	Data message modification
Control packet precision	Control packet integrity	Sybil,message modification

From the above existing work, we can conclude (refer figure 5) possible security solutions according to the nature of the attack and their requirements. Moreover, we observe (refer table 1) that very few security solutions employ the trust concept. Table 1 clearly indicates the suggested security solutions with their advantages, disadvantages and complexity analysis.

Trust-aware security models have become a promising and exciting technique for BSNs since they impose less overhead than cryptographic algorithms. Trust models (TMs) for BSNs [2]–[7], [9], [10], [34], [35], [42], [43] are broadly classified in data TMs and node TMs [17], [19], which are further subdivided into centralized, distributed and hybrid TMs [1], [3], [6], [11]–[18], [51]–[54]. Centralized TMs are failed due to single point of failure, and distributed TMs incur high overhead. Hybrid TMs for clustered BSNs are a feasible solution [11]–[14] over-centralized and distributed TMs in terms of accuracy, overheads, cost, convergence [51]–[53]. Moreover, there exist various basis of trust computation in TMs such as weight-based, rate-based, fuzzy-based, Bayesian, entropy-based, game theory, etc [3]–[6], [9], [26], but weight-based TMs seems to be an effectual and reliable solution for BSNs since it is small network [40], [42] where weights can be adjusted according to patient condition [3], [5], [6], [27]. Furthermore, weight-based TMs enforce less complexity [50]–[55] than other bases of trust computations.

III. PROPOSED LIGHTWEIGHT TRUST–AWARE SECURITY SCHEME FOR DECISION MAKING

In this section, we discuss a multifactor (direct and indirect communication trust, data trust, energy trust, weight, and frequency of misbehavior) based TM to prevent the WBAN from the aforementioned internal attacks. The projected TM (ETAS) is a distributed TM in which each biomedical SNs compute the trust value of other SNs and generate data packets. Relay nodes are used to forward trust values or data packets towards the sink node. Figure 6 shows the key steps of proposed ETAS to make it clearly understandable.

The distributed approach is suitable for the small networks [2], [3], [11] since less number of sensor nodes (10-100) incurs low communication overhead. This section is classified into four subsections. The first subsection discussed network topology and various assumptions made in the proposed work. The second subsection assigns unique labels to each biomedical sensor node to make communication easier. The third subsection discussed the core part of the research work that is the trust estimation function. The fourth subsection discuss hotspot node detection algorithm which incorporate temperature of relay nodes, trust values as well as residual energy of SNs to make effective decision.

A. NETWORK MODEL AND ASSUMPTIONS

In our system, we incorporate three types of biosensor nodes, namely the intelligent physiological sensors (IPS), the relay nodes and the sink nodes. In the first type, intelligent physiological sensors collect and process the sensitive data from the patient body.

It has ability to monitor the body health indicators and to generate data packets of the measured data with limited hardware, software and power capabilities. We presume that the IPSs are implanted on the human body, (i.e., patient) in a distributed way where an IPS may be either biomedical SN or relay node that can interact (forward trust values) using multi-hop communication. Relay nodes are trusted devices used to forward trust values or data packets towards another relay node or sink node. Relay nodes usually have high sensing power than biomedical SNs as well as estimate temperature level of neighbor relay nodes by counting the packets transmitted and received. We assume sink node (BS) is a central command authority and cannot be captured by adversaries. Moreover, it can find and replace faulty IPS for the adequate functioning of the remote healthcare system.

Sink nodes are highly trusted and resource efficient nodes that transmit the aggregate sensitive health data to the medical staff for issuing appropriate command. The relay nodes are

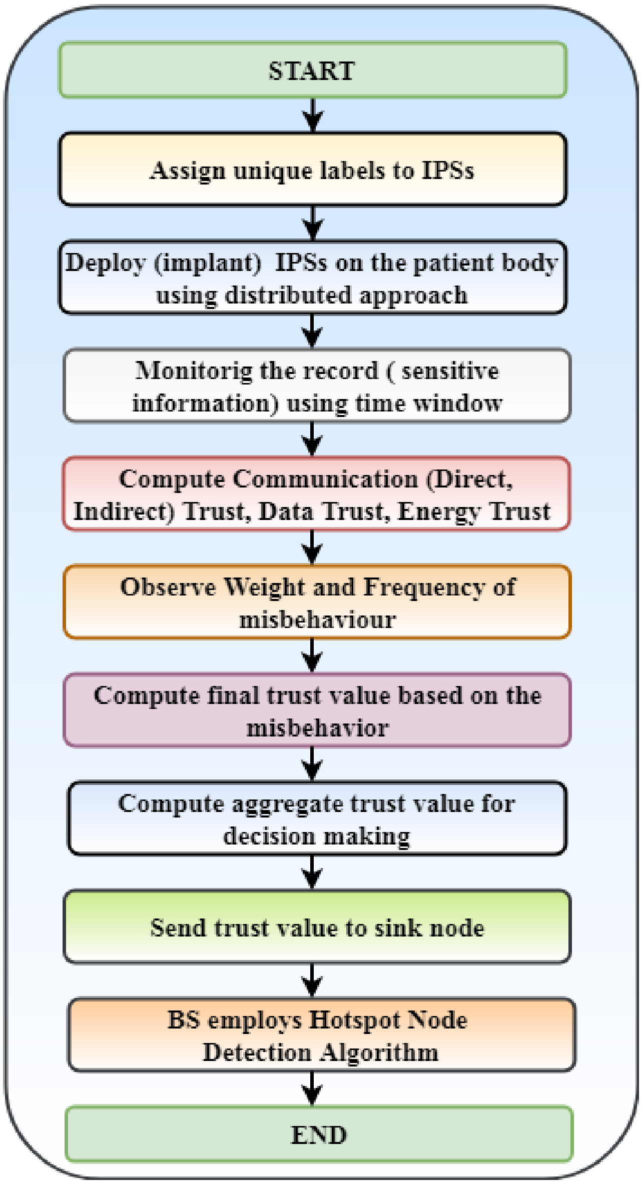
START
Assign unique labels to IPSs
Deploy (implant) IPSs on the patient body using distributed approach
Monitorig the record (sensitive information) using time window
Compute Communication (Direct, Indirect) Trust, Data Trust, Energy Trust
Observe Weight and Frequency of misbehaviour
Compute final trust value based on the misbehavior
Compute aggregate trust value for decision making
Send trust value to sink node
BS employs Hotspot Node Detection Algorithm
END

FIGURE 6. Key steps of ETAS.

TABLE 2. Comparative analysis and observation of various trust-based schemes for WBANS.

Trust model	Key objectives	Advantages/ Methodology	Limitation	Complexity
[2]	Trust-based secured multicast scheme	Prevention from faulty IPSs, uses historical trust records, residential time, reward and punishment concept to obtain precise trust values ,efficient data transmission using multicast approach, validation using theoretical and experimental results	Centralized trust model, residual energy as well as data trust of IPSs are not measured during trust computation, not robust against numerous internal threats, collaborative attacks are possible	Acceptable (Moderate)
[9]	Incorporation of trust and reputation schemes in BSN to progressthe efficiency of an evidence-based trust model against collusion attack	incorporating trust awareness into beacon-based location tracking for BSNs by introducing a new uncertainty based trust scheme	Neither robust nor comprehensive, don't consider the weight of misbehavior during on-off mitigation, not suitable for BSNs	Minimal
[3]	Distributed Trust Model to detect malicious IPSs	Application Independent, uses HELLO message and node community concept, direct trust, historical trust, recommended trust to obtain final trust value	Static trust function, data trust is not considered during final trust computation, no punishment to malicious nodes, not consider misbehavior frequency	Acceptable (Moderate)
[5]	Subjective logic trust evaluation, analyzing the behavior of nodes using sensor readings	inspect the quality of sensor reading by employing decay function and uncertainty, less memory overhead	Non-scalable weighted approach, week opinion aggregator, suitable for few threats	Acceptable (Moderate)
[10]	Designed a multi-party authenticated key agreement protocol known as GDP to establish initial trust.	based on symmetric-key cryptography, not rely on any supplementary hardware appliance, supports fast batch deployment	Not robust against internal security threats, no trust computation method, no load balancing, don't focus on fundamental requirements of BSNs	High (due to cryptographic scheme)
BAN-Trust [34]	Recommendation-based Trust Management, identify the malignant attacks	Not employ encryption techniques, Cosine-based similarity metric and user-based collaborative filtering is used to check similarity in recommendation vectors and computation of recommendation trust respectively, conceives the common behavior between the nodes,collect the information for trust assessment.	Not robust, not employ data trust and node misbehaviors rate and frequency, static trust function, no punishment and reward concept, doesn't conceive the energy of the nodes	Minimal
[6]	fuzzy trust model for public key distribution, mitigate malicious behavior to improve reliability, guaranteed key validation, reduce query traffic	Compute nodes trust value by using fuzzy sets, employs the concept of trusted neighbors to access public keys by assigning ranks, direct and indirect trust is estimated for decision making	Data trust and node misbehavior frequency is not computed for decision making, static trust function	Minimal
[7]	trust-based access control model, user behavior-based trust scheme	User trust computing involves trust evidence acquirement and trust aggregation, weighted approach	problem of combining behavior evidence for user-behavior trust evaluation, not robust, attack analysis is missing	Moderate
[35]	Trust-aware lightweightencryption scheme, primary focus on user-centric privacy-preserving and information security	Social multi-trust management, effective for Eavesdropping attack, Tracking attack, Spoofing attacks,etc	Suitable for a small set of attacks, various attacks are not discussed, don't focus on dependability issue	High (due to authentication scheme)
[42]	trust-based intrusion detection model(IDS), identify the spiteful nodes	Clustered approach, transmit the energy-effective data, consider triple trust (cooperative trust, data trust, and energy trust).	Simple trust function, not robust against conflict behavior attack, etc.	High
[43]	Trust-based lightweight security model, discover delay contributed IPSs, focus on data freshness	Incorporation of delay factor in trust evaluation to find secured routing path in the multi-hop environment, employ Beta distributions	Linear trust function based on only direct trust, no punishment and reward concept, indirect trust and energy trust are not considered,	Minimal
PSTRM [24]	first sociopsychological model, compute direct and indirect trust	High detection rate of faulty nodes, allotment of truthful indirect trust information within WSN	Susceptible to various security threats, employ cryptographic algorithm which impose computational overhead	High

selected based on the distance from the sink and residual energy of sensor nodes. A node having shortest distance from sink node as well as having highest residual energy is selected as relay node.

Moreover, we incorporate a logical time window [52]–[54] to monitor patient health (physiological activities) at regular intervals (say (Δt)) for accurate decision-making. It contains recently experienced information and drops older information for the effective cure of remote patients since recent health activities are more important than older information. WBANs are usually static [1]–[3] as IPSs are implanted on the same patient body at all times. Here, we are not focusing on memory overheads since storage capacity within IPSs is sufficient [34]–[38] to hold a patient health record that was a severe issue in ordinary WSNs deployed in a hostile environment. [10]–[12] can be used to secure the communication channel. To reduce the transmission and power overhead [17], we consider a flexible domain (say Đ) of trust values where Đ $\in$ [0 10]. Although any splendiferous range can be set but [17], [18] suggest lower range results in low overhead during the exchange of trust values.

1) ADVERSIAL MODEL AND POTENTIAL SECURITY ATTACKS

We discuss a node misbehavior based adversary model for internal security threats. In this adversary model, a selfish node constantly monitors the behaviors of other IPSs and messages transmitted within the network. During the interaction, malicious nodes increase/decrease the trust rating of other IPS by falsely recording more/less number of successful interactions. Moreover, a malicious IPS provides negative feedbacks of other IPS to degrade the network performance. Furthermore, a malicious node tries to manipulate the recorded data and sent it to reliable nodes to increase its temperature due to unnecessary processing for long time. An adversary periodically changes its behavior to misguide the genuine IPSs with the prospect that malicious behavior will be undetected. Our adversary model considers attack during frequent interaction of IPSs and attack during no interaction (or less interaction) of IPSs. We examine possible scenarios of the adversary model as follows

Scenario 1: When the nodes are interacting frequently and sharing information with each other. It may be a possibility the either sender node or receiver node may be a malicious node that drops the data packets, report false data or tries to change the content of data packet. This scenario can be handled (identified) by computing the communication trust and data trust as discussed in trust assessment scheme of proposed work.

Scenario 2: When the nodes are interacting less frequently and showing high trust values. This scenario can be handled (identified) by computing the non- cooperative interaction based trust calculation. We compute the weight and frequency of misbehavior.

Scenario 3: When a Sybil node tries to misguide the network. This scenario can be handled (identified) by verifying the assigned IDs and location of the nodes that is recorded in a matrix at the time of deployment. Later, we apply trust assessment scheme to analyze the behavior of nodes. If final trust value is less than threshold then base station will remove the spiteful IPS.

Scenario 4: When a spiteful IPS tries to waste the network resources or increase the temperature of reliable nodes by unnecessary processing of false data. This scenario can be handled (identified) by hotspot node detection algorithm that uses temperature threshold, energy threshold and final trust value as input to produce output.

ETAS system classifies the malicious parties into outsider adversaries (external attacker) and insider adversaries (internal attacker). External attacker tries to modify/eavesdrops the transmitted message by observing the communication channel within the BAN system. It may be active or passive attacker. The insider adversaries are the unreliable parties such as biosensor nodes within the system. The unreliable biosensors perform intentional malicious activities (i.e. report false data, drop packets) to degrade the performance of BAN system. However, these malicious internal nodes are limited in their processing capabilities and time. We consider the following attacks in our system:

a: BADMOUTHING ATTACK

A malicious IPS intentionally provides the negative feedback to evaluating IPS about evaluated IPS to demolish its reputation within the BAN. The negative feedback may be packet non-forwarding nature, high energy consumption during packet processing, non-optimal route selection to forward received packets. Due to these negative feedbacks, packets are forwarded to long route through unreliable IPS to waste the energy of BAN and disrupt the entire network.

b: BALLOT-STUFFING ATTACK

A malicious IPS falsely increases the trust value of other faulty nodes to raise their reputation in the BAN for degrading the performance of the network.

c: SYBIL ATTACK

A malicious IPS creates multiple fake pseudonymous identities to control and influence the entire BAN system. It is a massive destructive attack that misleads the other genuine IPS by showing their duplicate ID to achieve high trust values with positive feedback. It occurs during information broadcasting and degrades data integrity, network lifespan, and resource utilization.

d: TRAITOR ATTACK

A malicious IPS gain high trust value by fairly interacting with reliable nodes for a while and later misuse the gained trust values to degrade the reputation of trusted IPSs.

e: GRUDGE ATTACK

A malicious IPS become a legitimate member of the network through another reliable node of the network by convincing him. Moreover grudge attacker take revenge from other reliable nodes by providing low trust score who gave him a low trust value.

f: WHITEWASHING ATTACK

An IPS with a low-trust score leaves the network and rejoin the network with a new identity to reset its reputation.

g: ON-OFF ATTACK

Malevolent IPSs can opportunistically behave alternatively well or poorly, compromising the BAN with the expectation that malicious behavior will be undetected.

B. ASSIGNING UNIQUE LABELS (IDs) TO IPSs

Different (unique) labels (i.e. IDs) to each IPSs plays a significant role in providing security from external attacks such as spoofing attack as well as makes communication easier. To generate unique labels (UL) for each IPS, we employ a hashing technique which takes a random number (say r') a key (say k) as follows

$$UL = ((k \oplus r'||H((k+1) \oplus ID||r') \qquad (1)$$

These unique IDs and location of the IPSs are stored in a vectored for verification purpose at the time of deployment.

C. TRUST ASSESSMENT SCHEME

After investigating several recent trust proposals(refer related work and table 2), we found the considerable shortcomings in existing TMs such as static TM without any punishment, non-adaptive, delay response, high overhead, temperature unaware, non-flexible without severity analysis.

Most of the WBAN TMs incorporate exhausted data (information) in decision making leads to uncovering (non-detection) of numerous symptoms of severe decease.

A robust TM must focus on the primary requirements of WBAN and offer flexibility in terms of adjusting some parameters (severity coefficient) such as reward and punishment for good and bad IPSs. The thorough explanation of the proposed TM (ETAS) is provided in the following subsections. Figure 7 shows the flow chart of proposed trust estimation approach. Furthermore, table 3 provide the description of notations used in the proposed work.

1) COMMUNICATION AND DATA TRUST CALCULATION

This section discusses the trust computation process based on the interactions among biomedical sensor nodes. If the biosensors are interacting frequently then we defined it cooperative interactions otherwise non-cooperative interactions. If the numbers of past communications are equal to or exceeding the interaction threshold, in that case we apply a success rate based dynamic approach in which domain of trust values, penalty and incentive can be regulated according to the demand of real-application and system requirements. On the other hand, if numbers of past interactions are less than to interaction thresholds, then we compute current and aggregate misbehavior along with weight and frequency and of misbehavior to isolate hotspot nodes.

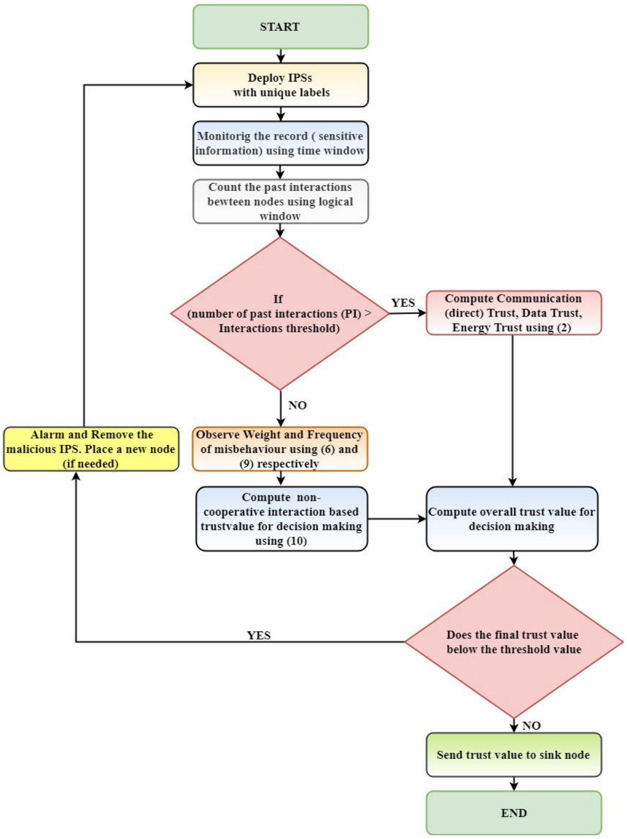
START
Deploy IPSs with unique labels
Monitorig the record (sensitive information) using time window
Count the past interactions bewteen nodes using logical window
If (number of past interactions (PI) > Interactions threshold)
YES
Compute Communication (direct) Trust, Data Trust, Energy Trust using (2)
NO
Observe Weight and Frequency of misbehaviour using (6) and (9) respectively
Compute non-cooperative interaction based trustvalue for decision making using (10)
Compute overall trust value for decision making
Does the final trust value below the threshold value
YES
Alarm and Remove the malicious IPS. Place a new node (if needed)
NO
Send trust value to sink node
END

FIGURE 7. Flow chart of proposed approach.

Cooperative Interaction (i.e. Success Rate) Based Trust Calculation: The communication (cooperative) trust and data trust of bio-medical SN(say y) at bio-medical SN(say x) during $\Delta t(T^{C,D}_{x,y}(\Delta t))$ when number of past interactions (PIs) is greater than or equal to interaction threshold is defined by (2). Equation (2) computes the communication (C) trust when biosensors are frequently interacting and exchanging monitored private data. Moreover, it is used to compute data (D) trust between the communicating biosensors. A successful data report between two biomedical sensor nodes (say x and y) is also verified by comparing the difference of data values reported with an error tolerance parameter (ξ). The error tolerance parameter is an error threshold for the data values reported by the bio-medical sensor nodes. It helps to identify the faulty nodes that are misbehaving with private physiological information.

$$\begin{aligned} &T^{C,D}_{x,y}(\Delta t)) \\ &= \left[Đ \times \left(\frac{S^{C,D}_{x,y}(\Delta t) + 1}{\left(S^{C,D}_{x,y}(\Delta t) + U^{C,D}_{x,y}(\Delta t)\right) + 2} \right) \right. \\ &\qquad \left. * \frac{1}{\sqrt{*(U^{C,D}_{x,y}(\Delta t) + 1)}} * \left\{ 1 - \frac{1}{S^{C,D}_{x,y}(\Delta t) + 1} \right\}^{\alpha} \right] \qquad (2) \end{aligned}$$

TABLE 3. Notations (symbols) used in ETAS.

Symbol	Meaning
$\mathrm{S}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})$	Successful Interactions of bio-medical SN x with bio-medical SN y during (Δt)
$\mathrm{U}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})$	Unsuccessful Interactions of bio-medical SN x with bio-medical SN y during (Δt)
$\mathrm{T}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t}))$	Communication trust and data trust of bio-medical SN (say y) at bio-medical SN (say x) during Δt
Ð	Domain of trust values
Γ	Punishment Coefficient
α	Reward Coefficient
Ø	Trust threshold
ρ	Application Specific Adjustable parameter
Δt	Time Window Consisting of 5 Time Units
$\mathrm{M}^{\mathrm{current}}_{\mathrm{x,y}}(\Delta\mathrm{t}))$	Current misbehavior of a bio-medical SN (say y) at bio-medical SN (say x) during Δt
$\mathrm{M}^{\mathrm{aggregate}}_{\mathrm{x,y}}(\Delta\mathrm{t}))$	Aggregate misbehavior of a bio-medical SN (say y) at bio-medical SN (say x) during Δt
f	Forgetting factor
r_i	Rate of misbehavior at i^{th}unit of time
$M^{weight}_{\Delta\mathrm{t}}$	Weight of misbehavior within time (Δt)
L	Number of time units in a time window (Δt)
$M^{frequency}_{\Delta\mathrm{t}}$	Misbehavior frequency
$T^{Misbehaviour}_{x,y}$	Final trust value based on the misbehavior
E_{th}	Energy threshold
E_{res}	Residual energy
E_c	Energy consumption rate
T_E	Energy trust
γ	Weight factor
ψ	Regulating factor
n	Total number of bio-medical SNs

where Δt is the time window consists of several time units whose length can be adjusted depending on network scenario. This logical time window adds newer experiences and forgets older experiences with the time elapses. Moreover, it helps to monitor good and bad behavior of biomedical sensor nodes. Superscript C, D denote communicationas well as data interactions and [.] denote the greatest integer function. $\mathrm{S}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})$ and $\mathrm{U}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})$ denotes cooperative and non-cooperative interactions used in the proposed work. Parameters Γ can be tuned according to application requirement to give harsh punishment with the increase in (non-cooperative) unsuccessful interactions. The first term $\frac{\mathrm{S}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})+1}{\left(\mathrm{S}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})+\mathrm{U}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})\right)+2\Big)}$ shows predictability trust which is a bayesianformulation using a beta reputation system. The second term $\frac{1}{\sqrt{*(\mathrm{U}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})+1)}}$ is punishment term whose value depends on the parameter Γ when there are no unsuccessful interactions (i.e.$\mathrm{U}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t}) = 0$) between SN x and y. The linear term $1 - \frac{1}{\mathrm{S}^{\mathrm{C}}_{\mathrm{x,y}}(\Delta\mathrm{t})+1}$ slowly tends to 1 withan increase in $\mathrm{S}^{\mathrm{C}}_{\mathrm{x,y}}(\Delta\mathrm{t})$ indicates a small alteration in the trust value of node x for node y. The exponent parameter $\alpha \geq 1$ is a reward parameter that gives the harshness to the trust function whose value can be adjusted according to network scenario and application requirement and plays a significant role to cope with untrustworthy nodes with greater values of reward parameter α.

Based on the communication and data trust values obtained by (2), a biomedical sensor node is categorized into three potential states as follows using (3).

$$S\left(\mathrm{T}^{\mathrm{C,D}}_{\mathrm{x,y}}(\Delta\mathrm{t})\right) = \left\{\begin{array}{c|l} (\rho\%\ of\ Ð;\ Ð) & highly\ trusted\ node \\ (0;\ Ø) & malicious\ node \\ (Ø;\ \rho\%\ of\ Ð) & legitimate\ node \end{array}\right\} \tag{3}$$

where the parameters Ø is trust threshold whose value is considered as one-third of maximum trust value (Ð/3). Equation (3) provide the trustworthiness status of communicating IPSs at Δt time period. It categories an IPS into one of three possible states namely highly trusted node, legitimate node and malicious node. The parameters ρ, and Ð are the adjustable parameters whose values can be regulated according to actual applicationrequirements or network scenario. This approach provides full flexibility in adjusting the trust value as well as a threshold value of trust using the application variable ρ.

2) NON- COOPERATIVE INTERACTION BASED TRUST CALCULATION

When biomedical sensor nodes do not frequently interact within specified time, i.e., when number of past interactions (PIs) is less than interaction threshold then instead of computing indirect (feedback) trust, we compute weight and frequency of misbehavior to isolate hotspot nodes since indirect trust are not able to catch on-off attack [1], collusion attack [9], etc. In addition, we use the previous communication trust score of SNs with aggregate misbehavior and current measured misbehavior to obtain robust current trust value of a node at time Δt. The current misbehavior (CM) of a bio-medical SN (say y) at bio-medical SN (say x) during Δt ($\mathrm{M}^{\mathrm{current}}_{\mathrm{x,y}}(\Delta\mathrm{t})$) is defined as follows using (4)

$$\mathrm{M}^{\mathrm{current}}_{\mathrm{x,y}}(\Delta\mathrm{t}) = \frac{\text{malicious behaviour}}{\text{malicious behaviour} + \text{expected (good) behavior}} \tag{4}$$

In order to analyze the persistency of misbehavior, we launch an aggregate misbehavior component as follows using (5)

$$\mathrm{M}_{\mathrm{x,y}}^{\mathrm{aggregate}}(\Delta\mathrm{t})) = \min\left\{ſ*\mathrm{M}_{\mathrm{x,y}}^{\mathrm{current}}(\Delta\mathrm{t}) + \left(1 - ſ\right) * \mathrm{M}_{\mathrm{x,y}}^{\mathrm{aggregate}}(\Delta\mathrm{t} - \Delta)), 1\right\} \quad (5)$$

where f is the forgetting factor that provide flexible weightage to the previous aggregate misbehavior.

As we know that biomedical sensor network deals with critical information of patients, so it is vital to analyze the weight of misbehavior after a fixed interval of time. The weight of misbehavior within time (Δt) is defined as follows using (6)

$$M_{\Delta\mathrm{t}}^{weight} = \max(ſ_1 r_1, ſ_2 r_2, ſ_3 r_3, \ldots\ldots\ldots ſ_i r_i, \ldots\ldots ſ_L r_L) \quad (6)$$

where L denotes the number of time units in a time window (Δt). The term $ſ_i$, r_i denote forgetting factor value as well as the rate of misbehavior at i^{th} unit of time. Note that $ſ_1 < ſ_2 < ſ_3 < ſ_4 < \cdots\ldots\ldots ſ_L$ which indicates our proposed approach assigns more weightage to recent misbehaviors rather than the older one that makes it a realistic approach. The rate of misbehavior for time unit (say i) as defined as follows using (7)

$$r_i = \left\{\frac{U_i}{S_i + U_I}\right\} \quad (7)$$

where U_i *and* S_i denote the number of malicious and good behaviors at time unit i. Since forgetting factor should increase with time so it must be dependent on the number of time units (L) in a time window as well as the current time period (i). The term forgetting factor ($ſ_i$) is defined as follows using (8)

$$ſ_i = \psi^{L-i} \quad (8)$$

where $0 < \psi < 1$.

In order to mitigate severe attacks, we integrate a new term known as misbehavior frequency ($M_{\Delta\mathrm{t}}^{frequency}$) to analyze the behavior of nodes in terms of the number of misbehaviors during some time period. To compute misbehavior frequency, we consider two time periods: active period ($A_{\Delta\mathrm{t}}$) and passive period ($P_{\Delta\mathrm{t}}$). Active period ($A_{\Delta\mathrm{t}}$) is defined as a time period when a particular node is misbehaving i.e. rate of misbehavior is greater than some specified threshold, and passive period is defined as a time period when a particular node is performing well. The frequency of misbehavior within time (Δt) is defined as follows using (9)

$$M_{\Delta\mathrm{t}}^{frequency} = \left\{\frac{A_{\Delta\mathrm{t}}}{A_{\Delta\mathrm{t}} + P_{\Delta\mathrm{t}}}\right\} \quad (9)$$

The history of misbehaviorfrequency is recorded in a logical array for decision making. It plays a vital role in the final trustworthiness evaluation of biomedical SNs. The final trust value based on the misbehavior ($T_{x,y}^{Misbehaviour}$) at time Δt is defined as follows using (10)

$$T_{x,y}^{Misbehaviour}(\Delta\mathrm{t}) = \left\{\begin{array}{ll} Đ * (1 - M_{\Delta\mathrm{t}}^{weight}) & \mathit{if}\ M_{\Delta\mathrm{t}}^{weight} > M_{\Delta\mathrm{t}}^{frequency} \\ Đ * [\gamma * (1 - M_{\Delta\mathrm{t}}^{weight}) + (1 - \gamma) & \\ \quad * \left(1 - M_{\Delta\mathrm{t}}^{frequency}\right) & \mathit{otherwise} \end{array}\right\} \quad (10)$$

Using (2) and (10), a hotspot (malicious) node can be accurately identified as follows using Algorithm 1.

3) ENERGY TRUST

Energy trust is defined as "the belief of one biomedical sensor node that other biomedical sensor node still has adequate energy to perform its intended function". We believe that selfish biomedical SNsneeded extra energy toinitiate severe selfish behaviors with the aim of destroying credibility of BAN. First we define energy threshold E_{th} and estimate residual energy (E_{res}) of biomedical sensor node. After estimating the value of E_{res}, we evaluate energy consumption rate (E_c) which depends on ray projection method [21]. We assume that with stable environmental conditions, energy consumptions rate of SN is stable. The energy trust (T_E) of a biomedical sensor node is defined using (11)

$$T_E = \begin{cases} 0 & \mathit{if}\ E_{res} < E_{th} \\ 1 - E_c, & \mathit{else} \end{cases} \quad (11)$$

The absolute trust value is computed by taking the average of communication trust, data trust, final trust value based on the misbehavior ($T_{x,y}^{Misbehaviour}$) and energy trust (T_E).

D. HOTSPOT NODE DETECTION ALGORITHM

In this subsection, an efficient multifactor hotspot node detection algorithm is discussed to detect malicious nodes in BANs. The hotspot node detection algorithm is a last step towards node's reliability that incorporates temperature of biomedical sensor nodes, absolute trust value and residual energy of nodes to make correct decision about the status of a node. We assume that during every packet forwarding, the temperature of a relay node is increased by 0.1 units. According to algorithm, if temperature of relay node (say i) is greater than equal to temperature threshold or absolute trust value is less than trust threshold or energy level of a node is less than energy threshold then node (i) will be hotspot node otherwise it is a reliable node. Once a node is detected as a hotspot node, base station eliminate this node from the network to improve the network lifespan since hotspot nodes consumes more energy to spread false information.

IV. RESULTS AND DISCUSSION

This section discussed the theoretical analysis and experimental results to prove the validation of recommended trust management scheme against BAN's attacks. In theoretical analysis, a logical and contradiction approach is being used to prove the robustness of ETAS. The detailed description of

Algorithm 1 Hotspot Node Detection Algorithm

```
Input: temperature of nodes, absolute trust values, trust threshold, energy, energy threshold
Output: hotspot node
Step 1.
∀ packet forwarding, Temp = Temp + 0.1 unit.
Step 2.
    If (temperature of relay node (i) ≥ temperature threshold) || (absolute trust value < trust threshold) || (energy level of a node < energy threshold)
        then
            node (i) hotspot node
        else
            If (temperature of relay node (i) < temperature threshold) && (absolute trust value ≥ trust threshold) && (energy level of a node ≥ energy threshold)
                then
                    node (i) is a reliable node
```

both (theoretical analysis and experimental results) isin the following subsections.

A. THEORETICAL ANALYSIS

Theorem 1: In node to node trust assessment as well as decision making, ETAS is potent against the selfish behavior of biomedical sensor nodes.

Proof (by Contradiction): Suppose a node (say y)fruitfully deceived another node (say x) then $U^{C,D}_{x,y}(\Delta t) \geq S^{C,D}_{x,y}(\Delta t)$ and $T^{C,D}_{x,y}(\Delta t) \geq$ Ø where the parameters Ø is trust threshold whose value is considered as one-third of maximum trust value (Đ/3). There exist three cases for this selfish behavior

Case 1: if node (x) and node (y) do not interact with each other, i.e., $U^{C,D}_{x,y}(\Delta t) + S^{C,D}_{x,y}(\Delta t) = 0$ then Eq.(10) incorporate misbehavior component and forgetting factor to caught its malicious behavior.

Case 2: if $S^{C,D}_{x,y}(\Delta t) = 0$ and $U^{C,D}_{x,y}(\Delta t) \geq 1$ then $T^{C,D}_{x,y}(\Delta t) = 0$ using Eq. (2). If number of interactions are less than interaction threshold then Eq.(10) will compute the trust value.

Case 3: if node (x) and node (y) interact at least once within (Δt) time i.e., $U^{C,D}_{x,y}(\Delta t) + S^{C,D}_{x,y}(\Delta t) > 1$ and $U^{C,D}_{x,y}(\Delta t) \geq S^{C,D}_{x,y}(\Delta t)$ then the predictability trust term $\frac{S^{C,D}_{x,y}(\Delta t)+1}{\left(S^{C,D}_{x,y}(\Delta t)+U^{C,D}_{x,y}(\Delta t)\right)+2}$ will always be less than 50% (i.e., 0.5) and the value of $T^{c,d}_{x,y}(\Delta t)$ will be less than Ø for any value of α, which contradicts the hypothesis.

Theorem 2: In node to node trust assessment and decision making, ETAS is potent against on-off attack.

Proof (By Contradiction):

Case 1: When number of interactions ≥ interaction threshold

Suppose a malicious node (say y) provide false information regarding interactions (say x) then $S^{C,D}_{x,y}(\Delta t) \geq U^{C,D}_{x,y}(\Delta t)$ and $T^{C,D}_{x,y}(\Delta t) \geq$ Ø. In this case, the term $\frac{S^{C,D}_{x,y}(\Delta t)+1}{\left(S^{C,D}_{x,y}(\Delta t)+U^{C,D}_{x,y}(\Delta t)\right)+2} < 1$ and $T^{C,D}_{x,y}(\Delta t) <$ Ø. It proves that ETAS is potent against on-off attack.

Case 2: When number of interactions < interaction threshold

In this case, a selfish node will try to show its trust score greater than equal to trust threshold i.e. $T^{Misbehaviour}_{x,y}(\Delta t) \geq$ Ø. As the interactions are less, frequency of misbehavior will be less than weight of misbehavior. In this case, the value of trust $T^{Misbehaviour}_{x,y}(\Delta t)$ will be less than trust threshold Ø. It means ETAS is potent against on-off attack against on-off attack.

B. EXPERIMENTAL RESULTS

This section discussed about the severity analysis of the suggested trust function and experimental results on MATLAB to exhibit the effectiveness of proposed trust management scheme in terms of severity of trust values, energy efficiency, packet drop ratio, and malicious nodes detection under varying network size. We have compared our suggested trust model (ETAS) with PSTRM [24] and BAN-TRUST [34]. PSTRM [24] is the latest trust model that guarantees for high detection of malicious nodes under small network size such as telehealth application. BAN-TRUST [34] is specially designed for body area networks and exhibit good performance.

C. SIMULATION SETTINGS

MATLAB with a communication system toolbox is a simulation platform apt for low powered wireless network scenarios, such as WBAN and WSN. For the experiment setup, IEEE 802.15.6 wireless standard is being adopted. The mentioned standard provides a low power, short-range, and reliable channels for human body communication. Also, we consider the multi-hop topology for data transmission in WBANs. For data communication, cooperative strategies are adopted between bio-sensors. The initial residual energy of biosensors is considered 5 Joules, and the communication range of the proposed WBAN is considered between 2 → 100 meters. The remaining energy is estimated by subtracting the sum of energy consumption in transmission and receiving of packets from total energy. For the proposed setup IEEE 802.15.6 wireless standard is used, and for data forwarding, distributed topology is used. A Nordic (nRF2401A) radio transceiver is used because it is a low power transceiver. We considered the simulation time 100 seconds for the proposed scheme. For simulation, we generate some good and bad behaviors for each time unit of the logical time window to assess the performance of the ETAS. Relay nodes estimate temperature level of neighbor nodes by counting the packets transmitted and received. Table 4 shows the list of parameters used in implementing the proposed work to analyze the effectiveness of the suggested

TABLE 4. List of parameters.

Parameter/feature	Value
Range of biosensors	10-50 (variable)
Geographical Region	100x100 Meter
Communication medium	Wireless channel
Topology	Distributed/Random
Coverage	30 Meter
Initial energy of biosensor	5 J
Range of relay nodes	5-10 (variable)
Range of malicious relay modes	3-4 (variable)
Number of malicious nodes	8-10 (variable)
Number of sink node	1
Position of sink node	(50m,50m)
Transmission range of relay nodes	25 meter
Trust threshold (Ø)	10 /3
Temperature threshold	60
Domain (Đ)of trust values	0 to 10
Application adjustment variable (ρ)	60
Error tolerance parameter(ξ)	0.5
Number of time units (L) in a time window	5
Energy Threshold (E_{th})	20% of initial energy (E)
Weight factor (γ)	.5
Regulating factor (ψ)	[0 1]
α	2
Node Deployment	Fixed

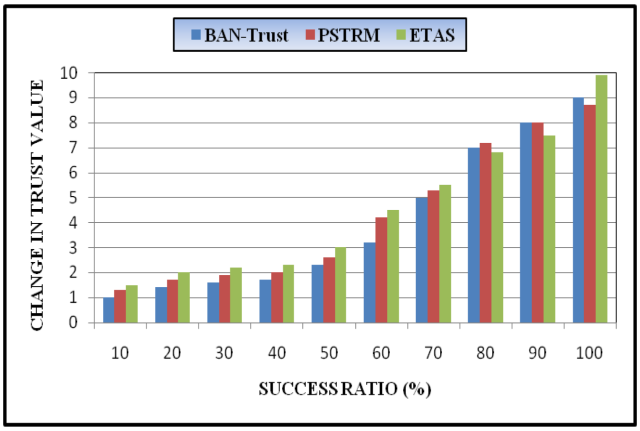

FIGURE 8. Success ratio vs. trust values.

approach (ETAS). Rest of the simulation setting for WBANs is described in [58], [61], [62].

1) EFFECT OF MALICIOUS NODES ON TRUST VALUE

In this subsection, we discuss the effect of malicious nodes on trust values. Figure 8 shows the effectiveness of ETAS in terms of success ratio and change in trust values of SNs. The term success ratio is the ratio of successful (cooperative) interactions to the total interactions. It is evaluated using the interactions recorded in the logical time window.

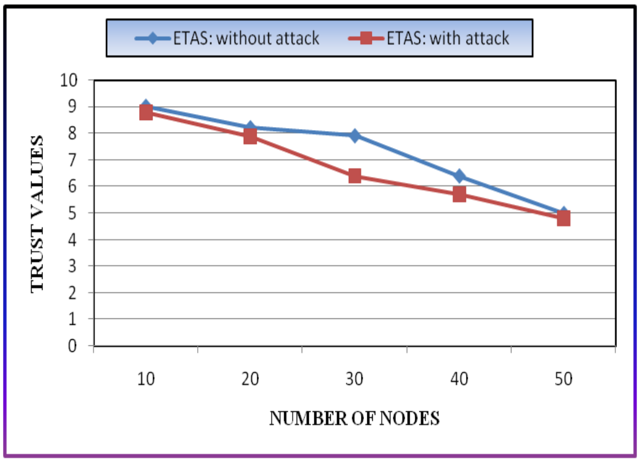

FIGURE 9. Effect of on-off attack on trust values.

When the numbers of cooperative interactions are increasing, the trust in EATS is gradually increasing. However in BAN-TRUST [34] and PSTRM [24], the trust value is not reaching to 10 with 100% successful interaction. Moreover, in PSTRM [24] the trust values are not gradually increasing with increasing cooperative interactions. The main reason behind the effectivenss of EATS is that its main focus is on interaction of nodes. EATS adopt appropriate trust evaluation strategy by counting the number of interactions between SNs. Furthermore, ETAS consider dynamic reward and punishment parameter along with misbehavior component to punish the selfish nodes. ETAS also has been tested by performing ballot-stuffing attack, whitewashing attack and on-off attacks since these attacks are very severe for patient's health related information. Figure 9 shows the effect of on-off attack on trust model. When the numbers of nodes are 10, 20, 30, 40, 50 then on-off attacks reduce the trust value by 0.2 (2.2%) , 0.2 (2.5%), 1.5(18.75%), 0.4(6.4%), 0.1(2%) respectively. The average change in trust values of genuine nodes is 6.37%. The accuracy of obtained information is 93.63% which is better than other existing trust models for BANs. However, we have analyzed combined effect of various attacks (ballot-stuffing attack, whitewashing attack and on-off) in figure 10. We intentionally inject upto 60% malicious nodes in BAN and found that ETAS perform better over BAN-TRUST [34] and PSTRM [24] due to robust trust model. Furthermore, we generate more selfish nodes to analyze the detection capability of ETAS, BAN-TRUST [34] and PSTRM [24]. The figure 11show that ETAS can effectively identify upto 92% malicious nodes in a network of 50 nodes since the hotspot node detection algorithm employs the temperature condition, trust value and residual energy of SNs.

The temperature and trust aware hot spot node detection algorithm minimize the risk of damaging sensitive tissues of a patient caused by high temperature of biomedical sensor nodes generated due to excessive communication.

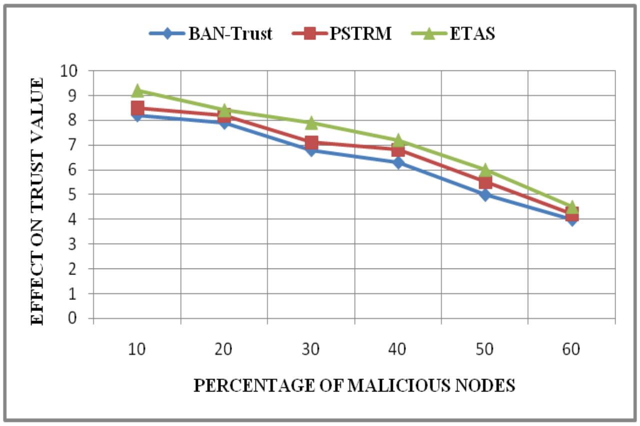

FIGURE 10. Effect of malicious nodes on trust values.

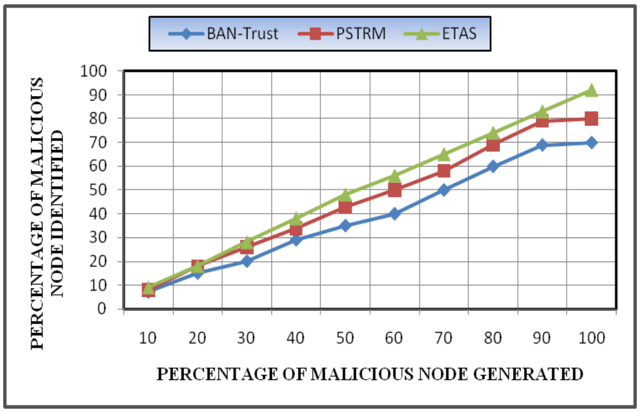

FIGURE 11. Malicious node detection.

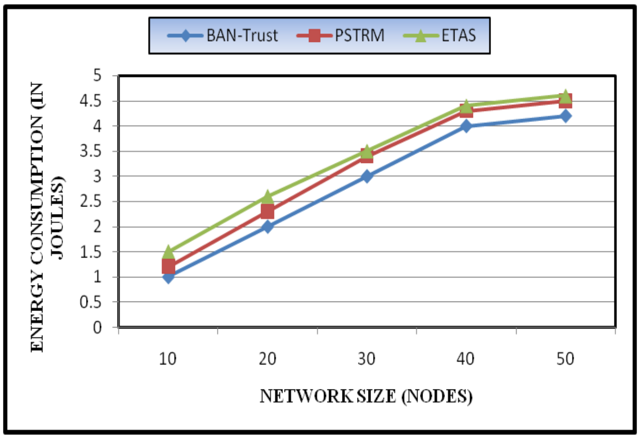

FIGURE 12. Analysis of energy consumption.

The Emulation result proves that ETAS is a great trust model that exhibits such great efficiency in terms of improving dependability and malicious node detection for BANs.

2) ENERGY CONSUMPTION

Figure 12 exhibits the energy utilization (in joules) of ETAS with [24], [34]. Energy consumption (utilization) is the amount of energy required to perform intended function during network lifespan. Mathematically, it is defined using (12):

$$Total\ Energy\ consumption = n * (E_t + E_r + E_i) \quad (12)$$

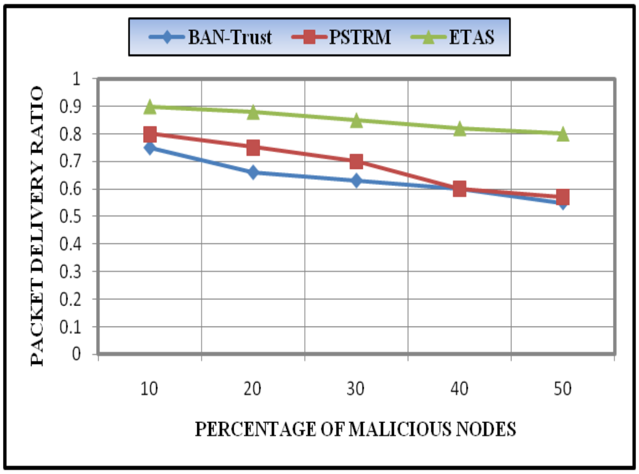

FIGURE 13. Effect of malicious nodes on packet delivery ratio.

where n is total number of biomedical SNs and E_t is energy required for packet transmission by a SN. The term E_r *and* E_i represent the energy required for receiving the packet and energy required for idling respectively. ETAS consume less energy than other existing trust model since computational complexity as well as bits required to store/process the trust values is minimal.

The ETAS performs 9% and 2.2% better over BAN-TRUST [34] and PSTRM [24] in terms of energy consumption. ETAS computational complexity largely depends on number of interaction among node.

D. PACKET DELIVERY RATIO

We have analyzed the effect of selfish SNs on the packet delivery ratio (PDR). The PDR is defined as the number of packets received by the base station (sink) successfully. Mathematically, it is defined using (13):

$$PDR = \frac{Total\ packet\ generated - total\ packet\ loss}{total\ packet\ transmitted} \quad (13)$$

Figure 13 shows that when numbers of selfish nodes are 10% then ETAS packet delivery ratio is 0.9 which is 11% *and* 16.66% better than PSTRM and BAN-TRUST respectively. Moreover, in a network of 50 malicious node, ETAS 32% and 34% better than PSTRM and BAN-TRUST respectively.

V. CONCLUSION

This paper presents a novel, weight based efficient trust assessment scheme (ETAS) for BANs that incorporate cooperative interaction based trust and non- cooperative interaction based trust values. ETAS is a temperature aware, interaction threshold based efficient trust assessment scheme for BANs. During cooperative interactions, ETAS computes communication trust and data trust between IPSs. Misbehavior component is used during non-cooperative interaction. During non-cooperative interactions, weight and frequency of misbehaviors are analyzed to punish the malicious IPSs.

ETAS is multi-factor trust assessment schemes that integrate triple trust namely communication trust, data trust and energy trust to determine the dependability status of a biomedical SNs. Relay nodes are selected based on remaining energy of nodes and distance from sink node. Finally, we present a hotspot node detection algorithm that effectively detects faulty nodes based on temperature, residual energy and trust values of sensor nodes. To the best of our knowledge, ETAS is the first trust assessment scheme that consider success rate and misbehavior component together depending on the interactions among the IPSs. The experimental results show the effect of percentage of successful interactions on trust value, effect of malicious nodes on trust value and packet delivery ratio (PDR). Furthermore comparative energy consumption is also analyzed. Finally the proposed trust assessment scheme (ETAS) is better than existing schemes in terms of malicious node detection, energy consumption, PDR and mitigation of spiteful nodes for healthcare applications. In future, we are planning to design a congestion aware trust-based secure system for BANs.

CONFLICTS OF INTEREST

The authors declare that they have no competing interests.

ACKNOWLEDGMENT

This work was supported by Universiti Kebangsaan Malaysia through the Prime Impact Fund (DIP) Grant under Grant DIP-2020-021. The Work is done in Secure Computing Laboratory, School of Computer and System Sciences, JNU, New Delhi.

REFERENCES

[1] H. Yu, Z. Shen, and C. Leung, "Towards trust-aware health monitoring body area sensor networks," *Int. J. Inf. Technol.*, vol. 16, no. 2, pp. 1–20, Jan. 2010.

[2] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 387–399, May 2009.

[3] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1164–1175, Nov. 2012.

[4] S. S. Javadi and M. A. Razzaque, "Security and privacy in wireless body area networks for health care applications," in *Wireless Networks and Security*. Berlin, Germany: Springer, 2013, pp. 165–187.

[5] V. Bui, R. Verhoeven, J. Lukkien, and R. Kocielnik, "A trust evaluation framework for sensor readings in body area sensor networks," in *Proc. 8th Int. Conf. Body Area Netw.*, 2013, pp. 495–501.

[6] G. W. Wu, Z. S. Liu, and P. Pirozmand, "A fuzzy trust model for public key distribution in body area networks," *Adv. Mater. Res.*, vols. 989–994, pp. 4837–4840, Jul. 2014.

[7] X. Wu, "A lightweight trust-based access control model in cloud-assisted wireless body area networks," *Int. J. Secur. Appl.*, vol. 8, no. 5, pp. 131–138, Sep. 2014.

[8] M. Ilyas, Z. Ullah, F. A. Khan, M. H. Chaudary, M. S. A. Malik, Z. Zaheer, and H. U. R. Durrani, "Trust-based energy-efficient routing protocol for Internet of Things-based sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 10, Oct. 2020, Art. no. 1550147720964358.

[9] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues," *IEEE Access*, vol. 6, pp. 17246–17263, Mar. 2018.

[10] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Trans. Sensor Netw.*, vol. 9, no. 2, pp. 1–35, Mar. 2013.

[11] T. Khan, K. Singh, L. H. Son, M. Abdel-Basset, H. Viet Long, S. P. Singh, and M. Manjul, "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks," *IEEE Access*, vol. 7, pp. 58221–58240, May 2019.

[12] N. Karthik and V. S. Ananthanarayana, "A hybrid trust management scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 97, no. 4, pp. 5137–5170, Dec. 2017.

[13] T. Kyung and H. S. Seo, "A trust model using fuzzy logic in wireless sensor network," *World Acad. Sci., Eng. Technol.*, vol. 42, no. 6, pp. 63–66, Aug. 2008.

[14] X. Wu, J. Huang, J. Ling, and L. Shu, "BLTM: Beta and LQI based trust model for wireless sensor networks," *IEEE Access*, vol. 7, pp. 43679–43690, Mar. 2019.

[15] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," *IEEE Access*, vol. 7, pp. 33859–33869, Mar. 2019.

[16] L. Yang, Y. Lu, S. Liu, T. Guo, and Z. Liang, "A dynamic behavior monitoring game-based trust evaluation scheme for clustering in wireless sensor networks," *IEEE Access*, vol. 6, pp. 71404–71412, Nov. 2018.

[17] R. Rani, S. Kumar, and U. Dohare, "Trust evaluation for light weight security in sensor enabled Internet of Things: Game theory oriented approach," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8421–8432, Oct. 2019.

[18] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wireless Netw.*, vol. 24, no. 3, pp. 777–797, Apr. 2018.

[19] N. Kumar, Y. Singh, and P. K. Singh, "An energy efficient trust aware opportunistic routing protocol for wireless sensor network," in *Sensor Technology: Concepts, Methodologies, Tools, and Application*. Hershey, PA, USA: IGI Global, Apr. 2020, pp. 628–643.

[20] M. S. Sumalatha and V. Nandalal, "An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN)," *J. Ambient Intell. Hum. Comput.*, vol. 12, pp. 1–15, Mar. 2020.

[21] J. Jiang and G. Han, "Survey of trust management mechanism in wireless sensor network," *Netinfo Secur.*, vol. 20, no. 4, p. 12, Jul. 2020.

[22] K. Yang, S. Liu, X. Li, and X. A. Wang, "DS evidence theory based trust detection scheme in wireless sensor networks," in *Sensor Technology: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, May 2020, pp. 321–334.

[23] M. E. Bayrakdar, "Cooperative communication based access technique for sensor networks," *Int. J. Electron.*, vol. 107, no. 2, pp. 212–225, Feb. 2020.

[24] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, "PSTRM: Privacy-aware sociopsychological trust and reputation model for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 13., no. 5, pp. 1–21, Sep. 2020.

[25] F. Ishmanov, S. Kim, and S. Nam, "A secure trust establishment scheme for wireless sensor networks," *Sensors*, vol. 14, no. 1, pp. 1877–1897, Jan. 2014.

[26] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "A survey on wireless body area network: Security technology and its design methodology issue," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2015, pp. 1–5.

[27] J. C. Weast, J. B. Cory, D. Vembar, and L. M. Durham, "Extension of trust in a body area network," U.S. Patent 14 573 992, Jun. 23, 2016.

[28] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 2, pp. 94–107, Apr. 2016.

[29] A. Joshi and A. K. Mohapatra, "Authentication protocols for wireless body area network with key management approach," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 2, pp. 219–240, Feb. 2019.

[30] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, Qua. 2014.

[31] H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in *Proc. 7th Int. Workshop Data Manage. Sensor Netw. (DMSN)*, 2010, pp. 2–7.

[32] M. Mana, M. Feham, and B. A. Bensaber, "Trust key management scheme for wireless body area networks," *Int. J. Netw. Secur.*, vol. 12, no. 2, pp. 75–83, 2011.

[33] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, May 2013.

[34] W. Li and X. Zhu, "Recommendation-based trust management in body area networks for mobile healthcare," in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2014, pp. 515–516.

[35] P. Guo, J. Wang, S. Ji, X. H. Geng, and N. N. Xiong, "A lightweight encryption scheme combined with trust management for privacy-preserving in body sensor networks," *J. Med. Syst.*, vol. 39, no. 12, pp. 1–8, Dec. 2015.

[36] T. Hayajneh, B. Mohd, M. Imran, G. Almashaqbeh, and A. Vasilakos, "Secure authentication for remote patient monitoring with wireless medical sensor networks," *Sensors*, vol. 16, no. 4, p. 424, Mar. 2016.

[37] G. Thamilarasu and A. Odesile, "Securing wireless body area networks: Challenges, review and recommendations," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Dec. 2016, pp. 1–7.

[38] A. A. Omala, K. P. Kibiwott, and F. Li, "An efficient remote authentication scheme for wireless body area network," *J. Med. Syst.*, vol. 41, no. 2, pp. 1–9, Feb. 2017.

[39] A. R. Bhangwar, P. Kumar, A. Ahmed, and M. I. Channa, "Trust and thermal aware routing protocol (TTRP) for wireless body area networks," *Wireless Pers. Commun.*, vol. 97, no. 1, pp. 349–364, Nov. 2017.

[40] N. S. Priya, R. Sasikala, S. Alavandar, and L. Bharathi, "Security aware trusted cluster based routing protocol for wireless body sensor networks," *Wireless Pers. Commun.*, vol. 102, no. 4, pp. 3393–3411, Oct. 2018.

[41] A. Chitra and G. R. Kanagachidambaresan, "Fault aware trust determination algorithm for wireless body sensor network (WBSN)," in *Proceedings 1st International Conference on Smart System, Innovations and Computing*. Singapore: Springer, May 2018, pp. 469–476.

[42] D. K. Anguraj and S. Smys, "Trust-based intrusion detection and clustering approach for wireless body area networks," *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 1–20, Jan. 2019.

[43] S. Roy and S. Biswas, "A novel trust evaluation model based on data freshness in WBAN," in *Proceedings of International Ethical Hacking Conference*. Singapore: Springer, May 2019, pp. 223–232.

[44] T. Wang, K. Hu, X. Yang, G. Zhang, and Y. Wang, "A trust enhancement scheme for cluster-based wireless sensor networks," *J. Supercomput.*, vol. 75, no. 5, pp. 2761–2788, May 2019.

[45] A. Ostad-Sharif, M. Nikooghadam, and D. Abbasinezhad-Mood, "Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks," *Int. J. Commun. Syst.*, vol. 32, no. 12, p. e3974, Aug. 2019.

[46] R. Nidhya and S. Karthik, "Security and privacy issues in remote healthcare systems using wireless body area networks," in *Body Area Network Challenges and Solutions*. Cham, Switzerland: Springer, 2019, pp. 37–53.

[47] S. Karchowdhury and M. Sen, "Survey on attacks on wireless body area network," *Int. J. Comput. Intell. IoT, Forthcoming*, vol. 3, pp. 1–7, Mar. 2019.

[48] M. Usman, M. R. Asghar, I. S. Ansari, F. Granelli, and M. Qaraqe, "Trust-based DoS mitigation technique for medical implants in wireless body area networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[49] S. R. H. Remu, M. O. Faruque, R. Ferdous, M. M. Arifeen, S. Sakib, and S. M. S. Reza, "Naive bayes based trust management model for wireless body area networks," in *Proc. Int. Conf. Comput. Advancements*, Jan. 2020, pp. 1–4.

[50] M. Roy, C. Chowdhury, and N. Aslam, "Security and privacy issues in wireless sensor and body area networks," in *Handbook of Computer Networks and Cyber Security*. Cham, Switzerland: Springer, 2020, pp. 173–200.

[51] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[52] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[53] S. Talbi, M. Koudil, A. Bouabdallah, and K. Benatchba, "Adaptive and dual data-communication trust scheme for clustered wireless sensor networks," *Telecommun. Syst.*, vol. 65, no. 4, pp. 605–619, Aug. 2017.

[54] M. Singh, A. R. Sardar, K. Majumder, and S. K. Sarkar, "A lightweight trust mechanism and overhead analysis for clustered WSN," *IETE J. Res.*, vol. 63, no. 3, pp. 297–308, May 2017.

[55] J. Górski and A. Turower, "A method of trust management in wireless sensor networks," *Int. J. Secur., Privacy Trust Manage.*, vol. 7, no. 3, pp. 1–19, Nov. 2018.

[56] B. Jiang, G. Huang, T. Wang, J. Gui, and X. Zhu, "Trust based energy efficient data collection with unmanned aerial vehicle in edge network," *Trans. Emerg. Telecommun. Technol.*, vol. 12, p. e3942, Mar. 2020.

[57] T. Li, W. Liu, T. Wang, Z. Ming, X. Li, and M. Ma, "Trust data collections via vehicles joint with unmanned aerial vehicles in the smart Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 4, p. e3956, Apr. 2020.

[58] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. M. Mohamed, "A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks," *IEEE Access*, vol. 8, pp. 131397–131413, Jul. 2020.

[59] S. Huang, A. Liu, S. Zhang, T. Wang, and N. Xiong, "BD-VTE: A novel baseline data based verifiable trust evaluation scheme for smart network systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Aug. 7, 2020, doi: 10.1109/TNSE.2020.3014455.

[60] S. Ramaswamy and J. Norman, "Social and QoS based trust model for secure clustering for wireless body area network," *Int. J. Electr. Eng. Educ.*, vol. 2020, Oct. 2020, Art. no. 0020720920953133.

[61] A. Samanta and S. Misra, "Energy-efficient and distributed network management cost minimization in opportunistic wireless body area networks," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 376–389, Feb. 2018.

[62] M. Alam, E. B. Hamida, D. B. Arbia, M. Maman, F. Mani, B. Denis, and R. D'Errico, "Realistic simulation for body area and body-to-body networks," *Sensors*, vol. 16, no. 4, p. 561, Apr. 2016.

ANAND KUMAR received the degree (Hons.) in mathematics from Osmania University and the master's degree in computer application and the M.Tech. degree from the School of Computer and System Sciences, JNU, New Delhi. He qualified master of computer application entrance exams of JNU, PUNE, DU, and HCU, and then joined JNU, in 1997. His prime research interests include body area networks, healthcare systems, and the Internet of Technology. He has experience of 16 years of teaching and research.

KARAN SINGH (Senior Member, IEEE) received the degree in computer science and engineering from the Kamala Nehru Institute of Technology, Sultanpur, India, and the M.Tech. degree in computer science and engineering from the Motilal Nehru National Institute of Technology, Allahabad, India, where he is currently pursuing the Ph.D. degree in computer science and engineering. He worked at Gautam Buddha University, from January 2010 to January 2014. He is currently working with the School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi. He supervised 35 master's degree students (M.Tech.) and four doctorate scholars. He published more than 80 research papers in the journal and good conference. His primary research interests include the computer networks, computer network security, multicast communication, and the IoT. He organized various workshop, session, conference, and training. Recently, he organized one week STC on "Network and Cyber Security" at Jawaharlal Nehru University. He is organizing the international conference on "Networks and Cryptology" at JNU. He has been a Professional Member of the Association for Computing Machinery (ACM), New York, the Computer Science Teachers Association (CSTA), USA, the Computer Society of India (CSI), Secunderabad, India, the Cryptology Research Society of India (CRSI), Kolkata, India, the Institute of Electrical and Electronics Engineers (IEEE), USA, the International Association of Computer Science and Information Technology (IACSIT), Singapore, the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST), USA, the International Association of Engineers (IAENG), Hong Kong, the Association of Computer Electronics and Electrical Engineers (ACEEE), India, the Internet Society (ISOC), USA, and the Academy and Industry Research Collaboration Center (AIRCC), India. He was nominated for Who's who in World, in 2008, and the IEEE MGM Award. He organized an International Conference Qshine 2013 as the General Chair. He worked as the General Chair of the International Conference QShine at Gautam Buddha University, in 2013. He is a reviewer of IEEE and Elsevier conferences and a reviewer of international journals and IEEE Transactions. He is an Editorial Board Member of *Journal of Communications and Network (CN)*, USA.

TAYYAB KHAN received the degree in computer science and engineering from Gautam Buddh Technical University, India, and the M.Tech. degree in computer science and engineering from the School of Computer and Systems Sciences, JNU, New Delhi, India, in October 2016, where he is currently pursuing the Ph.D. degree in computer science with the School of Computer and Systems Sciences. His primary research interests include the wireless sensor networks, network security, and multicast communication.

ALI AHMADIAN received the Ph.D. degree from Universiti Putra Malaysia (UPM) and the Ph.D. degree in 2014. He is currently a Senior Lecturer with the Institute of Industry Revolution 4.0, National University of Malaysia. He is an Adjunct Lecturer with Kean University, Wenzhou Campus, China. He is a Visiting Professor with the Mediterranea University of Reggio Calabria. As a young researcher, he is dedicated to research in applied mathematics. After his Ph.D. degree, he was a Postdoctoral Fellow at UPM. He was an Associate Researcher with the University of Malaya. He was promoted as a Fellow Researcher at UPM, in December 2017, and supervised a number of Ph.D. and M.Sc. students as the main and a member of supervisory committee. He was recognized by Google Scholar for the field of fuzzy sets and systems based on citations to his research works. In general, his primary mathematical focus is the development of computational methods and models for problems arising in computer science, biology, physics, and engineering under fuzzy and fractional calculus (FC). In this context, he has worked on projects related to nano-communication networks, drug delivery systems, acid hydrolysis in palm oil frond, carbon nanotubes dynamics, nanofluids, and viscosity. He could successfully receive 17 national and international research grants (Worth: $ 800, 000) and selected as the 1% top reviewer in the fields of mathematics and computer sciences recognized by Publons, during 2017–2020. He is an author of more than 80 research articles published in the reputed journals, including high prestigious publishers such as Nature, IEEE, Elsevier, Springer, and Wiley. He also presented his research works in 38 international conferences held in Canada, Serbia, China, Turkey, Malaysia, and United Arab Emirates. He was a member of program committee in a number of international conferences in AI at Japan, China, South Korea, Turkey, Bahrain, and Malaysia. He is a member of editorial board in *Progress in Fractional Differentiation and Applications* (Natural Sciences Publishing) and a Guest Editor in *Mathematical Methods in Applied Sciences* (Wiley), *Advances in Mechanical Engineering* (SAGE), *Symmetry* (MDPI), *Frontier in Physics* (Frontiers), and *International Journal of Hybrid Intelligence* (Inderscience Publishers). He is also serving as a referee for more than 80 reputed international journals.

MOHAMAD HANIF MD. SAAD received the B.Eng. degree (Hons.) in mechanical and materials engineering from Universiti Kebangsaan Malaysia, in 1999, the M.Sc. degree in mechatronics from the National University of Singapore, in 2001, and the Ph.D. degree in intelligent systems from Universiti Kebangsaan Malaysia, 2017. He is currently an Associate Professor with the Institute of IR4.0, Universiti Kebangsaan Malaysia. His research interests include intelligent systems, system integrations, the IoT, and complex event processing.

MANISHA MANJUL received the degree in computer science and engineering from KNIT, Sultanpur, India, the M.Tech. degree in computer science and engineering from NIT Jalandhar, India, and the Ph.D. degree in computer science and engineering from Gautam Buddha University, India. She worked at Gautam Buddha University. She is currently working with the Department of Computer Engineering, G.B. Pant Engineering College, New Delhi. Her primary research interests include computer networks, network security, multicast communication, and object-oriented programming. She is a Life Member of CSI, India.