IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 23, 2017, accepted February 13, 2017, date of publication February 22, 2017, date of current version March 15, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2672827

TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks

IDRIS ABUBAKAR UMAR[1], ZURINA MOHD HANAPI[1], (Member, IEEE), A. SALI[2], (Member, IEEE), ZURIATI A. ZULKARNAIN[1], (Member, IEEE)

[1]Department of Wireless and Communication Technology, Faculty of Computer Science and Information Technolog, University Putra Malaysia, Serdang 43400, Malaysia

[2]Research Centre of Excellence for Wireless and Photonic Network (WIPNET), Department of Computer and Communication Systems Engineering, Faculty of Engineering, University Putra Malaysia, Serdang 43400, Malaysia

Corresponding author: Z. M. Hanapi (zurinamh@upm.edu.my) and I. A. UMAR (brossadiq@gmail.com)

This work was supported by Research Grant UPM-FRGS-08-02-13-1364FR and the Tetfund through Kano University of Science and Technology, Wudil, Kano State, Nigeria.

ABSTRACT The cross-layering concept has enabled flexibility in sensor communication by decreasing the level of modularity through inter-layer information exchange. This has improved adaptability, reliability, and efficiency in the communication process. This is principally so, because the inter-layer information is utilized to enable the selection of nodes that are perceived to foster efficient communication. However, despite these numerous achievements, the cross-layering concept suffers immensely as a result of security attacks, which prey on nodes utilized for data forwarding. In this paper, we propose T-XLM, a trust-based cross-layering framework to provide minimal defense against security attacks. The framework introduces a fuzzy-based trust estimation mechanism, which is used to formulate imprecise empirical knowledge that is utilized for reputation building in the nodes to ensure secure forwarding and reliable delivery of data. We further proposed trust-based fuzzy implicit cross-layer protocol (TruFiX), a T-XLM inspired protocol which utilizes multiple parameters pulled through inter-layer information exchange to mitigate the effects of security threats in a network. Using extensive simulation experiments, TruFiX was compared with resource bound security solution (RBSS)-based protocols, which also achieved minimal security by altering their routing semantics. The conducted experiments evaluated the security performance of the protocols and the results show that the proposed TruFiX significantly outperforms the RBSS-based protocols in terms of packet delivery.

INDEX TERMS Wireless sensor networks, resource bound security, cross-layering, fuzzy logic system, blackhole, sybil.

I. INTRODUCTION

The cross-layering approach has succeeded in enhancing performance in Wireless Sensor Networks (WSN) due to their ability to pull system parameters from multiple layers needed to improve a target QoS metric. For instance, power control parameters from physical layers are combined with routing and congestion control parameters to improve on delay and lifetime of the network. Robust routing protocols, such as GPSR [1], CBF [2], IGF [3], XLP [4] just to mention a few, have been proposed using this cross-layering approach. The protocols offer significant improvements in terms of energy and QoS offered as compared to other traditional layered-based protocols. However, a comparative study performed on the cross-layering frameworks for WSN in [5] shows that most frameworks failed to consider the idea of a holistic security feature or mechanism despite its importance in todays networking and communication processes. Other attempts towards producing cross-layer protocols with security capabilities end up producing protocols with security at one (or at most two) of the layers, and yet, still struggle to conserve the constrained resources as the security mechanisms such as intelligent agent, key management module and database proposed in [6]–[8] respectively tend exert substantially on the resources. For instance, the key management mechanism employed for cryptography, when embedded into the routing protocols poses a greater problem due to cipher text message expansion results, which tend to consume memory, bandwidth, and energy when subjected to a multi-hop network where each relay node is expected to decipher and encrypt while maintaining the initial sender's cipher. This sort

of network suffers increased delay, shorter lifetime and in some instances zero delivery due to depleted nodes. For these reasons, the trust-based systems are seen as an alternative to traditional security towards secure data delivery in a treat-based WSN.

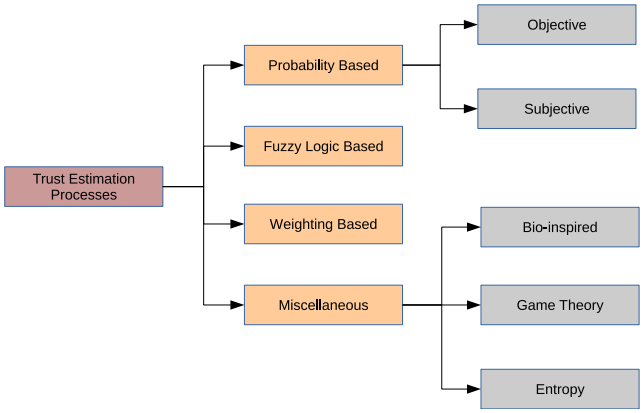

FIGURE 1. Trust Estimation Processes.

Trust in its literal meaning is defined as the belief or expectation or assurance of sincerity, competence, and integrity transacting entities have on each other [9]. It has been utilized in the realm of network security to secure and manage interactions between entities or nodes. This is achieved by leveraging generated evidence produced from previous interactions, which are returned back as feedback, to enable the control of entities interactions. The trust concept, which emerged from control theory (closed loop feedback control mechanism), is fused with uncertainty and subjectivity. And as such, measures towards estimating the degree of acceptance (trust) of one entity to another have been devised using trust representatives (variables) and relationships connecting the transacting parties. In [9] and [10], trust estimation processes were categorized into four classes shown in Figure 1. Researches dealing with trust in WSN for security provision are currently on the rise. Technologies such as Internet of thing (IoT), cloud and Fog networks, which are utilized for surveillance, agriculture, medical monitoring, emergency response and big data analytics are currently exploring various possibilities in these research aspects. This is because the WSN consolidates these technologies. However, due to the layered structure of the sensor node, it is impossible to provide a protocol with holistic security solutions capable of thwarting all routing attacks in a network.

In this paper, we propose T-XLM, a cross-layer framework that considers a robust approach towards securing a sensor-based network. The framework utilizes a trust-based approach to accommodate and analyze information pulled from multiple layers using strict boundary conditions to initiate and coordinate entities interaction during an intimidated routing process. Our proposed framework builds on the novel unified cross-layer module (XLM), which is known for its excellent adaptable feature [11]. We further, proposed TruFiX, a configurable cross-layer protocol inspired by T-XLM. The protocol employs a fuzzy logic trust-based estimation process to enable and accommodate interlayer information exchange, configured to possess spatiotemporal and traffic awareness so as to ensure and enhance its security performance. Using extensive simulation experiments, the security performance of TruFiX and other secure cross-layer routing protocols (RBSS-based) was compared in the presence of blackhole and Sybil attacks. The results obtained show that the TruFiX achieves a higher performance in terms of packet delivery.

II. RELATED WORKS

A. THE XLM FRAMEWORK

In this section, we briefly discuss the XLM framework and how it maps its variables to the sensor protocol stack to achieve its unification. The XLM framework was developed to leverage the use of minimal available resources to achieve efficient communication. This was enabled by merging the most intrinsic protocol layer functionalities into a single module, which is utilized to implicitly provide the necessary requirements for successful communication. The XLM design is based around an initiative concept that provides complete autonomy to each node, as to when deciding on partaking in the communication process. The Initiative denoted as I_d as shown in equation 1, is set to 1 if the candidate node satisfies the all the four conditions and 0 if otherwise. The conditions are ascertained by variables which represent the intrinsic functionalities across the protocol stack and they include: received signal to noise ratio ξ_{RTS}, relay packet rate λ_{relay}, remaining buffer capacity β and remaining energy E_{rem}.

$$I_d = \begin{cases} 1 & \text{if } \begin{cases} \xi_{RTS} \geq \xi_{RTS}^{Th} \\ \lambda_{relay} \leq \lambda_{Th} \\ \beta \leq \beta^{max} \\ E_{rem} \geq E_{rem}^{min} \end{cases} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

The process of selecting a participating candidate node is termed Initiative Determination. The process is initiated whenever a source node announces its intention of forwarding a message of interest to a destination node. The announcement is sent to nodes as a Request-to-Send (RTS) broadcast. The candidates (nodes within broadcast range) on receiving the broadcast, begins to independently decide on participation by using the initiative determination selection process. Nodes contend to be selected as the forwarding candidates by transmitting a Clear-to-Send (CTS) reply together with values representing the initiative variables. The first variable ξ_{RTS} determines the link reliability between the candidate node and the source node, the second candidate variable λ_{relay} ensures traffic control which prevents congestion, the third variable β also prevents buffer overflow due to uncontrolled traffic and lastly, E_{rem}, ensures availability and survivability of a node through the period of communication.

The node that fulfills all the four criteria, as well as the spatial relay criteria is selected as the forwarding candidate.

TABLE 1. Main notations.

Notation	Definition
ξ_{RTS}	Received signal to noise ratio
λ_{relay}	relay packet rate
β	Remaining buffer capacity
E_{rem}	Remaining energy
I_d	Initiative determination
T	Trust
T	Trust-based initiative
R	Reputation
I	Modified Initiative determination
β_{op}	Buffer occupancy period
ω_{relay}	packet's waiting relay period
τ	data transfer duration
Sr	Success ratio
fr	fairness ratio
T_m^n	Trust of node m within node n
f and g	functions
ϕ	Traffic statistic
Ω	Traffic volume
$\alpha_1 - \alpha_6$	Traffic statistic determining parameters
∂_1, ∂_2	Traffic volume determining parameters

The XLM achieves significant energy savings using congestion control measures (in variable λ_{relay} and β), which mitigate packet loss that may lead to retransmission. Thus, providing a distributive, adaptable, and reliable communication model. Protocols classed as being inspired by this framework or ideas similar to this include XLP [4], which pulls parameters from physical, MAC, routing as well as a transport layer to form a unified decision incentive to determine a nodes willingness to participate in the communication process. EBGR in [12] that utilizes the physical, MAC and routing layer parameters to determine the next-hop relay by means of contention through the RTS/CTS handshaking and similarly MACRO [13], which only employs the MAC and routing parameters, just to mention a few. However, this initiative determination or contention based selection was not intended for the secure routing purpose, thus limiting protocols functionality to systems which are attack free.

Wood et al. in [14] using a contention based approach, proposed a family of configurable secure routing protocols (SIGF-0, SIGF-1, and SIGF-2) termed resource bound security solutions (RBSS). The protocols achieve security by altering the normal protocol semantics by employing a fixed collection window period. During this period multiple responses received from contending nodes in the form of parameters (MAC and routing parameters) are sampled within the given fixed window period. The node with the highest value based on the selection criteria set is chosen as the next hop node. The protocols SIGF-0, SIGF-1, and SIGF-2 were subjected to the blackhole, Sybil, and DoS attacks. The performance of SIGF-0, SIGF-1 and SIGF-2 were rated good, better, and best respectively, but at the cost of increasing complexity due to the installed mechanisms utilized for the security provision.

Similarly, Hanapi et al in [15] proposed DWSIGF to improve the security performance of SIGF-0 by using a random collection window period. The random collection window created spontaneity in the protocol semantics thus enabling the DWSIGF to outperform the SIGF-0 protocol when subjected to blackhole and Sybil attacks [16]. However, the spontaneity induced affected the normal workings of the protocol causing frequent retransmission whenever there is a failure in response capture from contending nodes during the random collection window period, thus causing increased energy consumption and end-to-end delay.

Umar et al in [17] proposed FuGeF to improve the security performance while maintaining QoS performance of DWSIGF. The authors propose the use of a fuzzy logic system to pull up MAC, routing, as well as physical layer parameters for analysis. They further introduced a restrained pseudo-random collection window period which maintains spontaneity while ensuring response capture. The protocol outperforms DWSIGF in terms of QoS performance and security performance when subjected to blackhole attack. On the other hand, no results were shown for Sybil attacks as with DWSIGF, this may imply that the protocol was tuned using the flexible fuzzy logic system to counter blackhole attacks only.

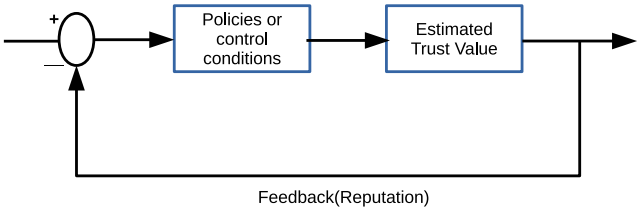

FIGURE 2. A typical trust model.

B. TRUST ESTIMATION PROCESSES

The concept of trust which originated from control theory was first proposed in the realm of E-commerce to select reliable transaction objects. Researchers proceeded by implementing the concept into different fields using modified policies to efficiently evaluate trust among the transacting entities as shown in Figure 2. Evaluation of trust is usually directly linked with past behaviors or indirectly combined with reputation passed from participating entities within a network [10]. Figure 1, shows four prominent classes of the trust evaluation/estimation processes commonly found in the literature.

The probability-based approach as seen in [18]–[22] was centered on the Bayesian probability and the Dempster-Shafer evidence theory. The approach is further categorized into two; The objective estimation which strictly depends on data analyzed from nodes (through direct observation) and the Subjective estimation which rationally changes on account of the evidence provided directly or indirectly as collected from nodes. The subjective estimation further introduced the nodes confidence level as a measure of the evidence analyzed from nodes [21]. Results obtained after the estimation adhere strictly to a fifty-fifty chance or binary outcome. For instance: a decision A (trustworthy if $P_{ij} > T_{def}$) or a decision B

(untrustworthy if $P_{ij} < T_{def}$), where P is a Bayesian probability function used to estimate the value of trust T and T_{def} is the defined threshold for T. This form of approach affects the performance of the network as there is small or zero flexibility in the decision made regarding the outcome obtained.

The works in [23]–[27] employed the fuzzy logic estimation approach for secure routing. Estimation of trust values here is concerned with the action of the entity such that an action could be rated positive or wrong to some degree [28]. The approach utilizes the membership degree and language variables, thus enabling flexibility, robustness, and ability to cope with uncertainty to the highest degree. The approach is capable of accommodating multiple variables from multiple layers for trust estimation. However, in some instances parameters or variables obtained from nodes have to be fine-tuned further using some form of calculations before being forwarded to the fuzzy logic system for processing. This increases the computational complexity. Also nodes variables representing a designated criteria or rules when poorly constructed can affect trust estimation process [10].

Weighting-based estimation is carried out by weighing the interaction of the communicating entities over a period of time. GMTS [29], PLUS [30] and [31] employed this estimation approach by attaching weighting factors to some of the variables to control and ensure that estimates are within an assigned threshold. Also, the approach uses formulated equations capable of accommodating multiple node parameters deduced from multiple layers for trust estimation. In some instances, a parameter is assigned a weighting factor to strengthen its degree of importance in the equation. The estimation approach is simple, easy to implement and has low computational complexity. However, the weighting factors (selected randomly) may affect the outcome of the estimation and parameter combination. Furthermore, the equations mostly employed for the trust estimation lack mathematical or statistical backing in theories or concepts.

Finally, the miscellaneous approaches are established using borrowed methods or inspired ideas from other scientifically and non-scientifically proven theories. Three of the most commonly utilized approaches comprise of the bio-inspired, entropy and game theory approaches. These methods, when adopted, tend to be less predictable due to the complexity of the prerequisites attached as it intends to initiate the estimation processes.

In this paper, we propose a T-XLM cross-layer framework, which is an extended version of the XLM framework. The T-XLM employs trust to determine a nodes incentive in partaking in the routing process. We further propose TruFiX, a T-XLM inspired protocol. The protocol employs 2-fuzzy logic systems for trust estimation. This estimation approach was employed due to its ability to accommodate multiple inputs, perform human-like decisions as well as cope with uncertainties to produce the most flexible scaled outcomes, such that trust are not interpreted as probabilities but rather as a gradual phenomenon similar to human interpretations. Thus, an entity is being trusted very much or more or less [28]. This interpretation has eliminated opinions that consider trust and distrust as opposite ends of the same continuous scale that are ill-equipped to differentiate a nodes weakness from malicious behavior. For instance, a node's congested buffer that often drops packet can be mistaken for a malicious behavior and marked distrusted despite it behaving in accordance with its best capacity.

III. THE PROPOSED T-XLM

This section presents the proposed T-XLM. It is intended to ensure secure node to node communication by utilizing information pulled from multiple layers of the sensor stack. The proposed T-XLM concept TI is described in equation 2, which is an associative relationship between the Initiative determination (I) and reputation (R). The modified process of the initiative determination (I) is shown in equation 3.

$$TI = I \otimes R \tag{2}$$

$$I = \begin{cases} Good, & \text{if } \begin{cases} \xi_{RTS} \geq \xi_{RTS}^{Th} \\ \omega_{relay} \leq \omega_{relay}^{Th} \\ \beta_{op} \leq \beta_{op}^{Th} \\ T \geq T^{Th} \\ E_{rem} \geq E_{rem}^{Th} \end{cases} \\ Fair, & \text{if } \begin{cases} \xi_{RTS}^{min} \leq \xi_{RTS} < \xi_{RTS}^{Th} \\ \omega_{relay}^{min} \leq \omega_{relay} < \omega_{relay}^{Th} \\ \beta_{op}^{Th} < \beta_{op} \leq \beta_{op}^{max} \\ T^{min} \leq T < T^{Th} \\ E_{rem}^{min} \leq E_{rem} < E_{rem}^{Th} \end{cases} \\ Unsuited, & \text{if } Otherwise \end{cases} \tag{3}$$

I is expressed in a form other than the binary. Additionally, ξ_{RTS} is the value of the received Signal to Noise Ratio (SNR) of the RTS broadcast determined from received SNR ξ_{RTS}, ω_{relay} is the rate of packets relayed by a node determined by the waiting time of packets receiving the RTS broadcast, and β_{op} is the buffer occupancy period. E_{rem} is the residual energy of a node.

$$R = \begin{cases} \text{Trusted}(T \geq T^{Th}) & \text{if } \begin{cases} Sr \geq Sr^{Th} \\ fr \leq fr^{Th} \\ \tau \leq \tau^{Th} \end{cases} \\ \text{Uncertain}(T^{min} \leq T < T^{Th}), & \text{if } \begin{cases} Sr^{min} \leq Sr < Sr^{Th} \\ fr^{Th} \leq fr < fr^{max} \\ \tau^{Th} \leq \tau < \tau^{max} \end{cases} \\ \text{Distrusted}, & \text{if } Otherwise \end{cases} \tag{4}$$

R Represents the node reputation value which updates the trust T value. The Trust is computed in equation 4. Its presence in equation 3 stands for initialized T values, which is afterwards updated in equation 4 during subsequent iterations in the routing process. Furthermore, Sr represents success ratio to determine a nodes potential in packet delivery, fr is fairness ratio to ensure route alteration and τ measures

the data transfer duration. The terms on the right side of the inequalities in both equation 3 and 4 represent the associated threshold and ranges for the parameters. The ability of the T-XLM to nullify or mitigate the effect of attacks as well as ensure reliable communication is due to these constraints (inequalities on the right side) that define the Trust-based initiative.

Candidates reputation R are ranked trusted (if $T \geq T^{Th}$), uncertain ($T^{min} \leq T < T^{Th}$) and distrusted (if Otherwise), depending on the trust estimate employed from the chosen estimation process. The process employed by this proposed framework to determine each nodes individual trust value is analogous to [32], where through direct observation, a node n computes the trust value (T_m^n) of a node m within its radio range as function (f) of the traffic statistics (ϕ) and traffic volume (Ω) as shown in equation 5 :

$$T_m^n = f(\phi, \Omega) \tag{5}$$

The traffic statistics and traffic volume are parameters monitored for a one-hop neighbor, which can further be defined as shown in equation 6 and 7:

$$\phi = g(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6) \tag{6}$$

$$\Omega = h(\partial_1, \partial_2) \tag{7}$$

Where; α_1 = packets sent by m to n that are dropped by m
α_2 = total packets dropped by m
α_3 = packets dropped by m due to congestion
α_4 =packets dropped by m due to unknown reasons
$\alpha_5 = n's$ assessment of $m's$ priority to $m's$ self-packet vs. all other nodes packet
α_6 = packets forwarding delay by m
∂_1 = packets misrouted by m
∂_2= packets falsely injected by m.

In the proposed frameworks (equation 3 and 4), the constraints (inequalities on the right side) both emulate functions similar to the traffic and volume parameters needed to produce trust based values representing a node's layer functionality.

A. ROUTING PROCESS IN T-XLM

In this section, an explanation is provided for the routing process in the proposed T-XLM and possible attacks during the routing operations. The communication process begins with a channel reservation phase where the sending node broadcast a RTS packet which serves as a trigger to potential relay nodes to initiate the contending process. An attacker at this point can decide to consistently send such a broadcast to prevent other sending nodes from forwarding their packets as well as cause energy depletion in the nodes intending to contend. Estimating the duration of the received RTS broadcast signal as well as the number of times it was sent can help identify if the signal was propagated by a malicious entity or not.

Afterwards, nodes on receiving the broadcast begin the contending process by responding back with a Clear To Send (CTS) signal by piggybacking the parameters ξ_{RTS}, ω_{relay}, β_{op}, T, and E_{rem} after a time period. An attacker at this point can struggle for selection by rushing to present a suitable feedback values such as a shorter waiting time, link quality and so on, as its response. Appropriate selection in such instances is made when the CTS responses are determined using boundary conditions, such as a period lower than a certain threshold is disregarded or link quality above a certain threshold is chosen. In our proposed T-XLM, the parameters ξ_{RTS}, ω_{relay}, β_{op}, T and E_{rem} employed to weight a candidate node during the selection process are rated good, fair, or unsuited based on the values returned by the nodes.

The selected forwarding node is then allowed to proceed to the next phase, where data is transferred to it. On completion of the forwarding process, the sending node is analyzed under the parameters Sr, fr, τ and rated trusted, uncertain and distrusted. This analysis is done to determine nodes trustworthiness in the case of future unforeseen interactions. Attacks here include instances where some malicious nodes can decide to hold data, drop all or some certain chunk of the data before forwarding to hinder network performance. The proposed T-XLM, using boundary conditions set for each parameter pulled across multiple layer of a node, should be capable of detecting and mitigating the effect of attacks such as jamming, blackhole, sinkhole, grayhole, and Sybil just to mention a few. However, due to the rapid emergence of new security threat posing several kinds of attack to a network, our model is not (in its holistic nature) invulnerable to all attacks.

B. THE PROPOSED TruFiX PROTOCOL

In this section, details are provided for the proposed T-XLM inspired protocol. The protocol leverages a modified IEEE 802.11 DCF MAC and two fuzzy logic systems to create a feedback mechanism which the secure routing process depends on. The fuzzy logic systems are installed in both the channel reservation phase (during the modified initiative determination) and the packet exchange phase (for the reputation build-up). These two phases ensure secure selection of forwarding candidates used to route packets reliably to their destination.

1) THE CHANNEL RESERVATION PHASE

The channel reservation phase begins when the sending node S's NAV timer is zero and an idle channel is sensed for a DIFS time period. S sends an Open Request To Send (ORTS) signal constituting the S's location and the targeted destination to nodes within its broadcast range. The nodes within the broadcast range consist of the forwarding candidates (potential contenders within the 60-degree sextant area) and non-forwarding candidates. On receiving the broadcast, the non-forwarding candidates cancel their responses by setting their NAV timer in accordance with the basic IEEE 802.11 semantics to avoid interference. The forwarding candidates, on the other hand, set up a CTS response time, which on its expiry triggers the forwarding of each candidate, CTS response to node S.

For this protocol, we configure the collected response parameters to constitute a progressive distance value (d) indicating the distance between the contending node and the sending node S, CTS response time (ω), which is also a function of connection quality based on node distribution in relation to distance as well as additional waiting period due to inter-frame spacing (from 802.11 semantics) and the initial trust (T) values which by default is set to 0.5. This is in accordance with the trust establishment principles in numerous researches such as [20], [21], [33] just to mention a few. Uncertainty in all entities is considered normal at the start of the interaction. Trust values for the entities are re-established or updated as they engage in more interaction. Each node's response is processed through the first fuzzy logic system to deduce the appropriateness of the next forwarding candidate (good, fair or unsuited). The one with the highest output value is selected based on the fuzzy rules and membership function set to mimic the boundary conditions.

The choice in parameters utilized and estimation mechanism can be modified for this phase to tackle the different kinds of attacks intended. In our approach, the Buffer controls (β_{op}) and E_{rem} were also negelected so as to ensure fairness when comparing with the RBSS based protocols and to simplify fuzzy design as with every parameter, more rules will have to be implemented. With regards to the mechanism, a Multi-criteria decision system (MCDA) or a support vector machine (SVM) can be configured to estimate and produce an output which may determine the suitability of a node.

2) THE PACKET EXCHANGE PHASE

Once a forwarding candidate is selected, the data exchange phase is engaged. Data is forwarded from the sending node S to the forwarding candidate. On completion of data exchange, three more parameters are evaluated. Parameters which includes; forwarding success ratio Sr which is a measure of reliability in data delivery, Transfer duration τ which measures the time taken from the start of data exchange period to its completion in relation to number of packet moved within that time period. And fairness ratio (fr) which promotes the dispersion of next hop relay choices among similar performing neighbors. The parameters Sr, fr and τ are passed through a fuzzy logic system to determine the nodes reputation value (R) from equation 4. This value (R) is now considered as the nodes trust value (T) in subsequent interactions. However, The R value for a node which ensures delivery exceeds the initial 0.5 trust value assigned to nodes. Thus, if subsequent interactions should occur along the route, that particular node will be selected. For this reason we further introduced the *forced fairness process*.

The *forced fairness process* allows each node to keep a list of the nodes that participated in the routing process. A node chosen to participate in the forwarding process, if found to have participated in the process earlier is penalized (despite trusted) by reducing its fr and τ values so as to ensure it is not selected in the subsequent rounds. Similarly malicious nodes that have managed to succeed in participating more than once are also penalized using the forced fairness process. The entire routing process is summarized in Figure 3. The routing process is concluded in line with the 802.11 semantics ($ORTS \Rightarrow CTS \Rightarrow DATA \Rightarrow ACK$).

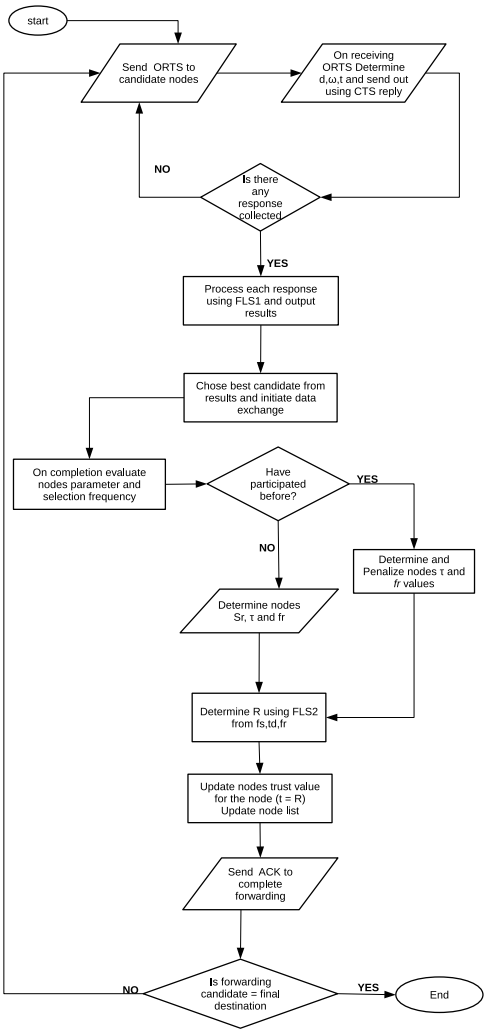

FIGURE 3. TruFiX Routing Process.

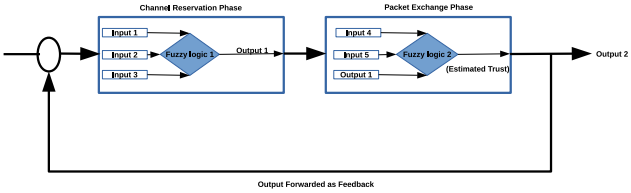

FIGURE 4. Proposed System Design.

C. THE FUZZY LOGIC SYSTEM (FLS)

In this section, details of the fuzzy logic design used for the routing process are presented. It should be noted that the overall trust-based initiative was achieved using both the two FLS. The output fed back into the system completes a single round of the trust-based initiative process shown in 4.

The need for FLS emerged due to the WSN constrained resources. It necessitates the need for a simple and fast decision-making system. The FLS is a computationally intelligent multi-valued logic system derived from fuzzy set theory to deal with reasoning, which is approximate rather than precise. Furthermore, the system is easy to implement and understand as it is based on natural language. Its ability to process and accommodate multiple inputs using minimal demand for memory and processing power deemed it preferable for WSN systems.

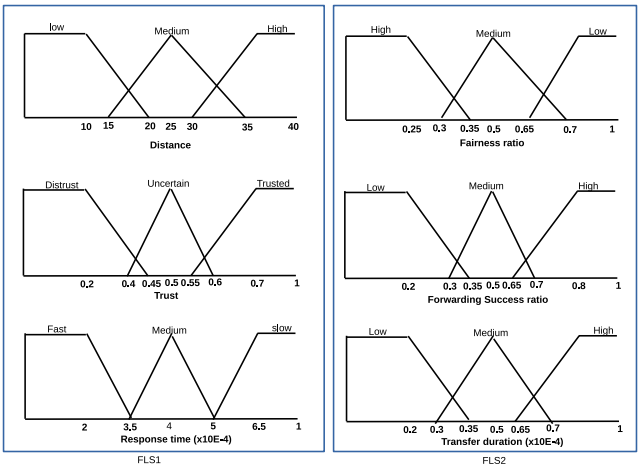

FIGURE 5. Input Membership Functions for TruFiX.

In the design of trust management system using the FLS, trust values are interpreted as an estimate inclined toward a degree of trust, uncertainty and distrust rather than probabilities taking a binary interpretation. The advantage of this kind of interpretation is the probabilistic interpretation fails in instances where the trust values fall within the threshold of absolute trust and absolute mistrust or uncertainty. But due to FLS humanistic intelligent decision, it is able to place a handle over such values. Figure 5 shows the proposed FLS membership function together with the universe of discourse of the two FLS.

It is worth noting that the parameters, membership functions, and rules are just a set of instances which if required can be extended and modified to suit the target experiments. The evaluation results could be more objective if input and output produced by the fuzzy logic systems are more fine-grained along with exhaustive and reasonable rule [33]. The choice of parameters utilized to tackle the kinds of attacks intended in this paper is shown in the FLS1 and FLS2 in Figure 5. Each FLS manages 3 of the parameters using 27 rules. In FLS1 distance, response time and trust are considered for processing to determine the appropriateness of a node. While fairness ratio, forwarding success ratio and data transfer duration are considered in FLS2. It should be noted that output produced from FLS2 for a node is returned as trust input of the node at FLS1, thus overwriting the previous default 0.5 initial trust value for that particular node. Also once the node is selected in subsequent routing operations, it undergoes the forced fairness process to prevent maintaining a single route, which eventually leads to energy depletion in the nodes along that route.

IV. PERFORMANCE EVALUATION

This section evaluates the performance of the RBSS based protocols and the proposed TruFiX protocol using MATLAB simulation. The protocols were evaluated in terms of Packet Delivery Ratio (PDR), possibility of attacker selection, end-to-end delay and energy consumption. The simulation was set up to emulate the type of traffic expected in low-bandwidth networks. Parameters employed for the setup included: radio bandwidth, payload size as well as Constant Bit Rate (CBR) set at 200kbps, 32bytes, and 100 packets, respectively. The terrain of 150 square meters containing 196 nodes each having a communication range 40m was prepared using a Gaussian distribution of 4m in standard deviation to achieve a grid-like node placement scenario. Table 2 summarizes the setting utilized.

TABLE 2. Simulation parameters.

Parameter	Value
Terrain	150 $times$ 150 m^2
Radio Range	40 m
Number of Nodes	196, Uniform
Node Placement	Grid +N (0,16)noise
Payload Size	32bytes
Radio Bandwidth	200 Kbps

The RBSS based protocols for our experiments are the DWSIGF and FuGeF. The protocols were chosen because they are both state-free cross-layer protocols which mimic initiative determination selection process (to some degree). Furthermore, the protocols possess resistance to routing attacks due to the absence of a routing table and a modified routing semantic. Our protocol design, though inspired by T-XLM still bases most of its assumption on the FuGeF protocol. However, FuGeF utilizes a single FLS with different parameters to achieve spatiotemporal awareness during the routing process. Its modified routing semantics ensures unpredictability and node capture to improve security and avoid retransmission problems as noticed in DWSIGF. For a detailed explanation on these RBSS based protocols refer to [16] and [17].

A. ATTACK-BASED NETWORK

1) ATTACK MODEL AND ASSUMPTIONS

In this paper, two forms of attacks were considered for the evaluation. The attacks which include: blackhole with CTS rushing attack and Sybil Attack. For both attacks assumptions made are;

- The network is assumed to be static and all locations are correct unless otherwise stated
- Source and destination nodes are trusted and attacker are found only within the relay nodes
- Attackers take up normal values and behaviors until selected for routing as they proceed to drop all data received

- The attackers are capable of analyzing a network's routing process both in timing and spatial orientation and can obtain and forward information regarding their vicinity and position of other nodes in the network.

2) THE BLACKHOLE WITH CTS RUSHING ATTACK

In this form of an insider attack, the attacker exploits the cooperative nature of the nodes by disregarding the protocols timing semantics during a CTS response period. The attacker in this instance rushes its CTS response after overhearing ORTS broadcast. This is to ensure it is included as a potential candidate with top values that might enable it champion through the needed selection process even if it does not fall within the forwarding area. If the attacker is selected, it drops all received packet. This reactive insider attack is very easy to perform but very devastating to a network.

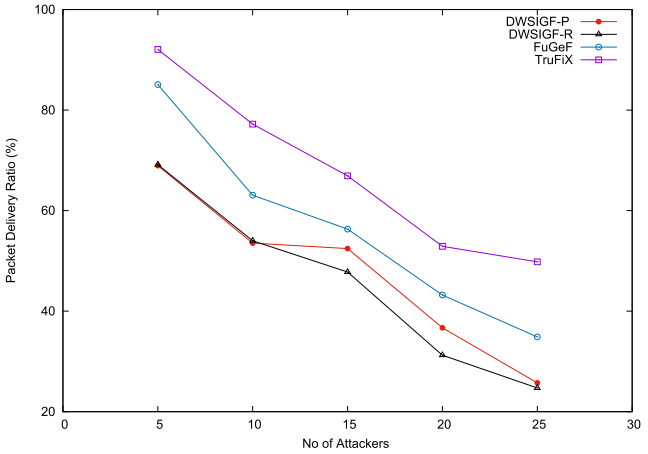

FIGURE 6. Packet delivery of randomly placed attackers.

In this paper, we test the impact of the attacker on two scenarios. The scenarios are similar to what was done in [17] for DWSIGF and FuGeF to ensure the validity of the work. The scenarios included:

1) *Random placement of attackers:* In this scenario, attackers were placed randomly in the network and increased (in number) in steps of fives (5) for each run . The experiment considered many-to-many mapping of which 6 sending nodes residing on the far left side of the network strive to forward the data of interest to 2 receiving nodes at the far right end of the network. Results shown in Figure 6 are the average of 100 simulation runs (for each step of 5) set for 7packet/sec Constant Bit Rate (CBR) flow. This experimental setting for many-to-many at this CBR traffic flow was chosen to mimic an adequately congested periodic point-to-point communication in such system
Figure 6 shows the graph of packet delivery ratio(%) against increasing number of randomly placed attackers using the blackhole with CTS rushing attack to exploit the network. DWSIGF-P and DWSIGF-R are variants of the DWSIGF protocol. The variants DWSIGF-P selects forwarding candidates that make that maximum progress towards their destination, which is the likes of the greedy forwarding strategy. On the other hand, the DWSIGF-R selects randomly from the forwarding candidates. The FuGeF protocol employs a single FLS to evaluate three parameters used to determine the forwarding candidates.
In this scenario, TruFiX outperforms the other three protocols and this was basically due to its ability to rate a node's performance using the second FLS (FLS2) as well as determine the participating frequency of a forwarding candidate. Its ability to penalize the malicious node and non-malicious nodes that have been utilized more than once was evident enough to prevent the malicious nodes from future participation in the routing process. Furthermore, its spontaneous route selection, which is similar to FuGeF was able to lower the chances of selecting the malicious nodes whose attack preys on the cooperative nature of the protocol.

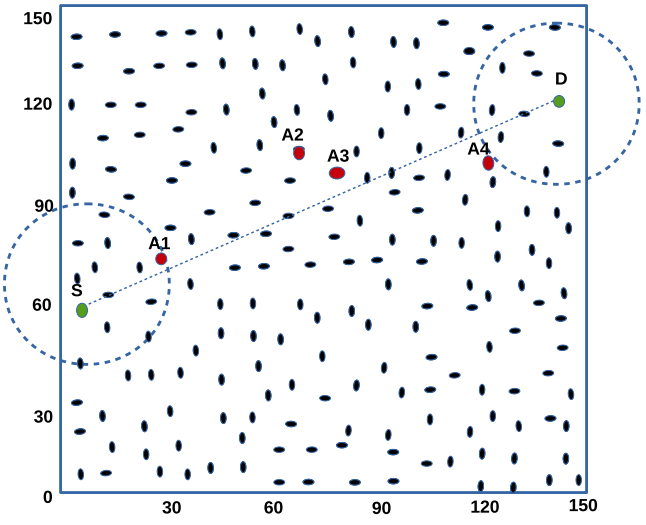

FIGURE 7. Strategic node placement.

2) *Strategic placement of Attackers:* In this scenario. The attacker(s) are placed at locations along the forwarding path. Locations are labeled A1, A2, A3 and A4 as shown in Figure 7. Location A1 and A4 are termed optimal position as they represent a position that has the highest correlation of being selected as the first and last hops, Location A2 and A3 are considered modal position because they represent the average correlation of being selected as middle hop nodes existing between nodes A1 and A4 [17]. The experiments in this scenario only considered one-to-one single CBR stream mapping of end-to-end nodes. It is worth noting that in such experimental settings, similar results are yielded for both one-to-one and many-to-many CBR traffic flows. The experiment further investigates through an average of a 500 simulation runs per location set for 7packet/sec CBR flow, the impact of the single and multiple

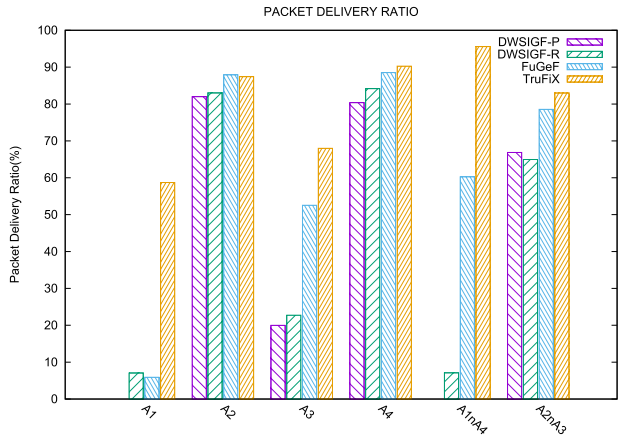

FIGURE 8. Packet Delivery for Strategically placed Attacks.

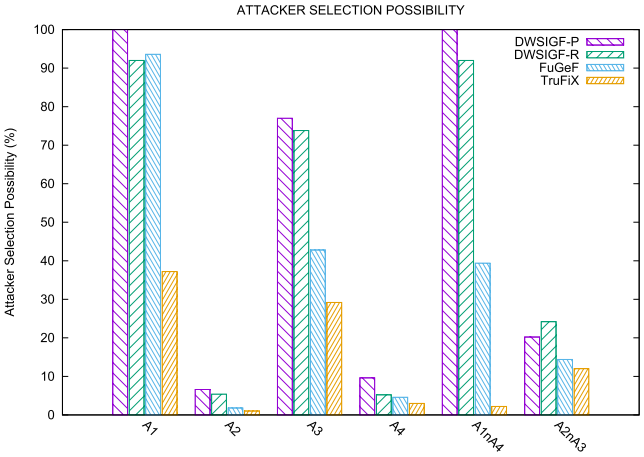

FIGURE 9. Possibility of Attacker Selection.

strategically located attacker(s) on the packet delivery and the possibilities of choosing the attacker(s) as shown in Figures 8 and 9.

In the first sub-scenario (A1), The attacker which is located in the optimal position was able (to some degree) to subdue the DWSIGF and FuGeF from bypassing its attacks, thus achieving 0%, 7% and 6% PDR for DWSIGF-P, DWSIGF-R, and FuGeF respectively. TruFiX, on the other hand, was able to attain 59% PDR as shown in Figure 8. Contrarily, attacker positioned at A4 (fourth sub-scenario), despite being an optimally positioned attacker had less effect on the protocols performance when compared to attacker placed at A1. DWSIGF-P, DWSIGF-R, FuGeF and TruFiX were able to achieve 80%, 84%, 88% and 90% PDR (Figure 8) with only 10%, 5%, 4.5%, 3% possibility of choosing the attacker (Figure 9), respectively.

In their combined attack (A1 and A4), in the fifth sub-scenario, the protocols which were fuzzy based were able to outperform the DWSIGF protocols. DWSIGF-P and DWSIGF-R maintained the same performance shown in A1 positioned attacks, while FuGeF and TruFiX achieved 60% and 95% PDR (Figure 8) with 40% and 2% possibilities of selecting the attackers (Figure 9), respectively.

In the case of the modal position, A2 (second sub-scenario is shown in Figure 8 and 9), the attacker had a small impact on the protocols. DWSIGF-P, DWSIGF-R, FuGeF and TruFiX were able to attain PDR of 82%, 83%, 88% and 87% and possibility of choosing the attacker of 7%, 5%, 2% and 1%, respectively. This was because the modal position A2 was easily bypassed during the node selection process. An attacker located at A3, on the other hand, has a higher frequency of being selected when compared to location A2. As such its impact (shown in the third sub-scenario) affected the protocols. DWSIGF-P, DWSIGF-R, FuGeF, and TruFiX achieved 77%, 74%, 43% and 29% in the possibility of choosing an attacker, which lead to 20%, 23%, 53%, and 68% PDR, respectively as shown in Figures 8 and 9.

In the combined attack of both A2 and A3 shown in the sixth sub-scenario, the protocols DWSIGF-P, DWSIGF-R, FuGeF and TruFiX attained PDR of 67%, 65%, 79% and 83% with 20%, 24%, 14% and 12% possibility of choosing the attackers respectively.

3) THE SYBIL ATTACK

The attacker (Sybil node) in this instance creates multiple nodes called virtual Sybil nodes. The nodes bear different identities and were placed on different locations along the routing path. Exploiting the cooperative nature of WSN, these virtual nodes on overhearing an ORTS signal, send their responses using proper identities enclosed. Once selected as the forwarding candidate, data exchange ensues. After which ACK is sent by the virtual node to the ORTS sender. However, the virtual attacker(s) in this experiment resorts to dropping all the received data.

In the experiments, we still maintained the one-to-one mapping to investigate the impact of six virtual nodes converging on the optimal or modal locations (A1 or A2 respectively) while increasing the traffic flow. The Sybil nodes positioned at A1 or A2 created the six virtual nodes so as to intercept responses and to ensure having more than a single candidate node during the node selection process. The identities of the virtual nodes were chosen to be identities other than the ones originally specified for the 196 legitimate nodes. The locations of the virtual nodes created were randomly assigned within a 25m radius (25m) from the Sybil node A1 or A2. Results produced are an average of a 1000 simulation runs/traffic flow.

Figures 10 and 11 show the result of the impact of a Sybil attacker located at A1, which created six virtual nodes randomly displaced within 25m to it. By presenting multiple identities the attacker increases its candidates during the selection period. Thus a substantial amount of the shared radio resources is allocated to these nodes. In addition to that, the virtual nodes can force network traffic to go through

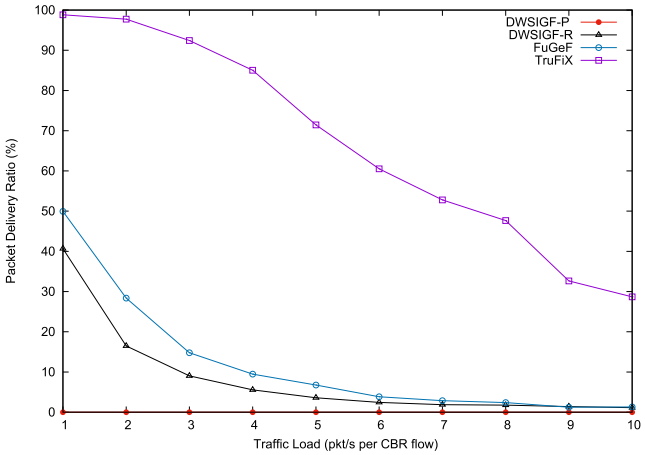

FIGURE 10. Impact of Sybil A1 on PDR.

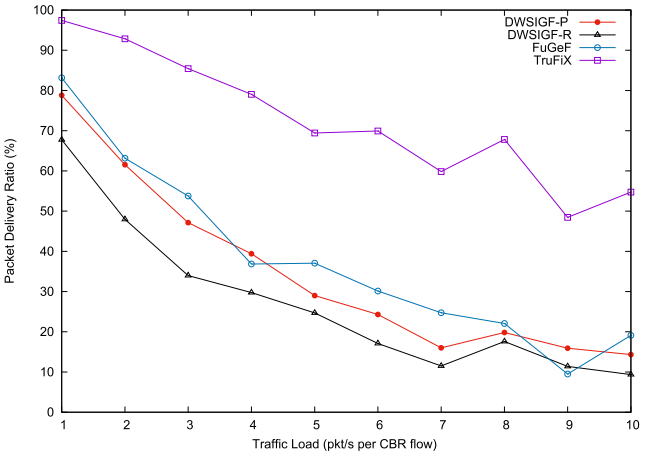

FIGURE 12. Impact of Sybil A2 on PDR.

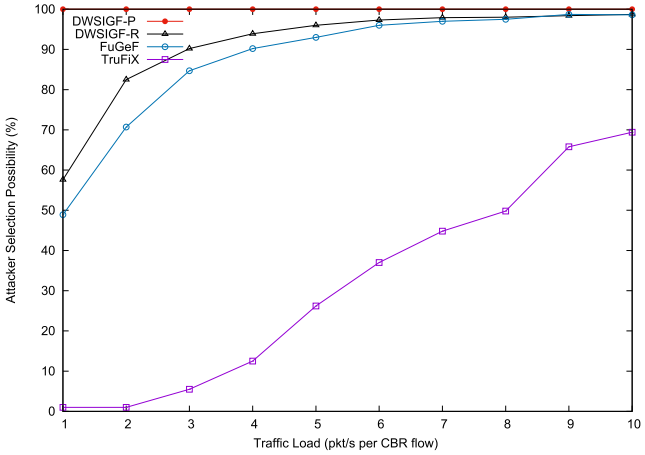

FIGURE 11. Impact of Sybil A1 on Selection Possibility.

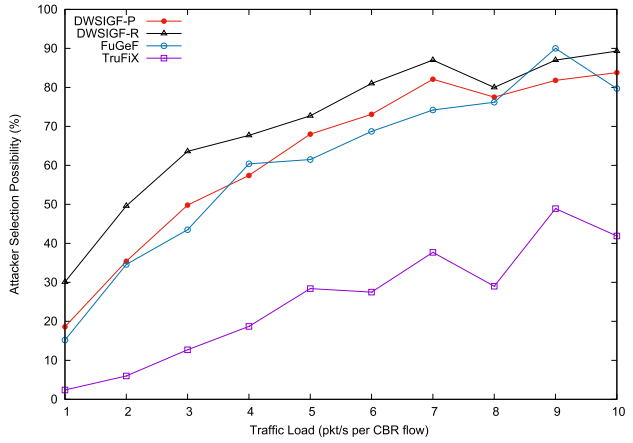

FIGURE 13. Impact of Sybil A2 on Selection Possibility.

a single node. This is what happens in the case of TruFiX. At lighter traffic flow, the non-malicious nodes utilized for forwarding were able to deliver as expected but as the traffic flow increased, they became congested and were forced to drop. This led to an overall average of 67% in its PDR as the attackers only attained an average of 31% chance of being selected. The impact of this Sybil attack worsened in the case of DWSIGF-P as the attacker had 100% chances of being selected. DWSIGF-R achieved an overall average of 8% PDR, as it ranged from 40% down to 1% as the traffic flow is increased. FuGeF, on the other hand, achieved an overall average of 12% in PDR and 88% chances of selecting the Sybil or virtual nodes during its selection. In TruFiX, The reputation built for the virtual nodes enabled the selection of the non-malicious nodes surrounding A1 which despite going through the forced fairness process, were selected in their congestive nature to deliver the packets.

The impact of the attacker located at A2 is shown in Figures12 and 13. The position, despite being easily bypassed, enabled the attacker to disrupt the forwarding process due to the spread in the virtual nodes (25m from A2). The DWSIGF-P achieved an overall average of 35% PDR with 63% possibility of selecting a malicious node, which in this instance, has outperformed DWSIGF-R with an overall average of 27% PDR and a 70% chance of selecting an attacker. FuGeF was slightly better than DWSIGF protocols as its PDR ranged from 83% down to 19% as the traffic flow was increased in steps of one. These lead to an overall average of 38% in PDR and 60% chance of selecting an attacker. TruFiX, on the other hand, outperforms all the three protocols as its PDR ranged from 97% down to 54% as the traffic flow is increased, achieving an overall average of 72% PDR and 25% possibility of selecting a malicious node.

These scenarios have demonstrated that the proposed protocol which utilizes two FLS to determine nodes trustworthiness when interacting with its entities can provide the best minimal security needed to defend against blackhole and Sybil attacks in a network.

B. ATTACK-FREE NETWORK (BASE PERFORMANCE)

We further tested the performance of the protocols in a threat free scenario. The experiment setup constituted many-to-many CBR flows from which 6 nodes from the far left side of the terrain are tasked with sending packets to 2nodes on the

far right of the terrain. Each of the two nodes is set to receive 3CBR flows from the sending nodes. Results shown in Figure 14 and 15 recorded an average of 100 simulation runs for each traffic flow for PDR and end-to-end delay respectively.

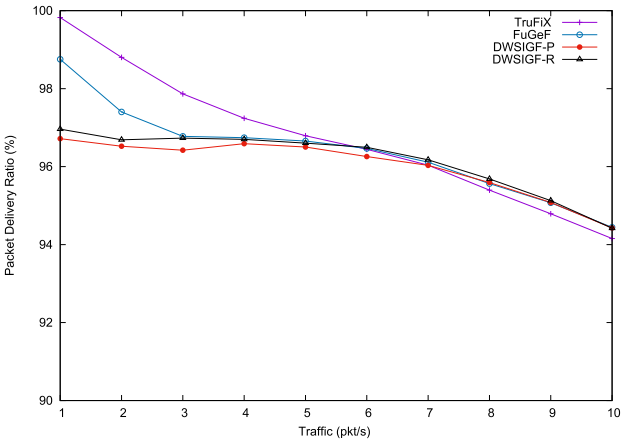

FIGURE 14. Packet Delivery Ratio.

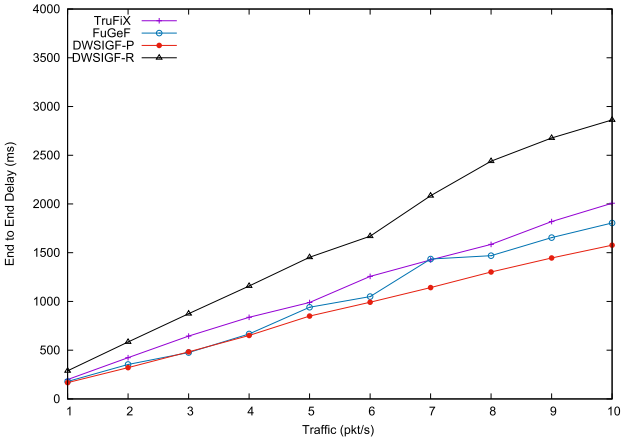

FIGURE 15. End-to-End Delay.

Figures 14,15 and 16 show the performance in PDR end-to-end delay and energy consumption of the protocols in an attack free network. TruFiX maintained higher packet delivery at lower traffic. This was due to its ability to select and maintain forwarding nodes that had a high forwarding success ratio (Sr). As the traffic flow increases, congestion and interference also increased. Nodes which had high forwarding ratios have been suppressed using the forced fairness process within the protocol semantics. These led to the selection of nodes that had less Sr values thus, aiding in substantial packet loss during the forwarding process. It is worth noting that in this design of TruFiX, parameters such as β_{op} and E_{rem} which have been neglected can be included in future implementations to remedy the substantial packet loss incured due to congestion. The TruFiX, however, due to the processing delays incurred by the two FLS and path dilatation caused by the forced fairness process, suffered increase in its

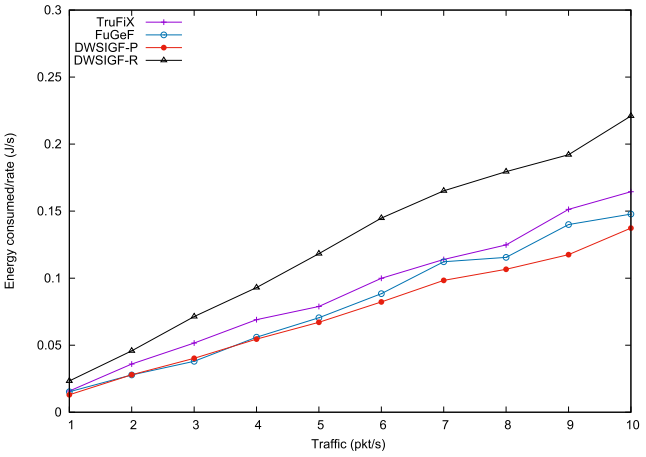

FIGURE 16. Energy Consumption.

end-to-end delay and energy consumption when compared to the FuGeF protocol.

The FuGeF also at lower traffic flows achieved higher PDR when compared to DWSIGF-P and DWSIGF-R. This was due to the forwarding node selection made by the FLS. The FLS ensured that nodes with links good enough to mitigate packet loss were chosen. But as the traffic flow is increased, congestion and interference increased in the network. FuGeF tries to maintain its performance by choosing nodes that are less prone to interference in order to abate packet loss. These, however, lead to an increase in the number of hops needed to reach the two far right nodes, which further increased the end-to-end delay and energy consumed as shown in Figure 15 and 16.

DWSIGF-P employs the greedy forwarding approach for its node selection. This has allowed it to utilize fewer numbers of hop in traversing the network. However, this selection strategy is prone to interference, thus hindering packet delivery as shown in Figure 14. On the other hand, DWSIGF-R chooses its forwarding candidate in a random manner. This selection since unpredictable, is able to choose nodes close to each other and in some instances nodes at the far end of the transmission range. Due to closeness (in proximity) of selected nodes (in some instances) interference is mitigated, hence the protocol is able to maintain packet delivery. However, higher number of hops are needed to traverse the network thus incurring increased end-to-end delay.

V. CONCLUSION

In this paper, we have proposed T-XLM, which is an improved version of the XLM framework that lacks provision for security. We further proposed a T-XLM based protocol TruFiX and it was compared with other secure protocols. The secure protocols (RBSS-based) achieved security by modifying their routing semantics to sample nodes in the case of DWSIGF and using fuzzy logic for node selection in the case of FuGeF. The proposed TruFiX, in addition to its node selection mechanism, included fuzzy logic based

trust estimation and forced fairness mechanisms to enable a distributed secure routing. Extensive simulation experiments were conducted to evaluate the effectiveness of these additional mechanisms in TruFiX. The result shows that TruFiX outperforms the RBSS based protocols in terms of security performance. This further implies that the proposed protocol achieves an optimally significant trade-off between security and other QoS metric in WSN. Future works will consider other forms of attacks and analysis of varying parameters to the FLS to determine the role parameters play in mitigating different forms of attack. The use of SVM and MCDA will also be applied to determine the effectiveness and efficiency of each estimation method on the routing process.

REFERENCES

[1] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. ACM 6th Annu. Int. Conf. Mobile Comput. Netw.*, 2000, pp. 243–254.

[2] H. Füßler, J. Widmer, M. Käsemann, M. Mauve, and H. Hartenstein, "Contention-based forwarding for mobile ad hoc networks," *Ad Hoc Netw.*, vol. 1, no. 4, pp. 351–369, 2003.

[3] S. Son, B. Blum, T. He, and J. Stankovic, "IGF: A state-free robust communication protocol for wireless sensor networks," Dept. Comput. Sci., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep., 2003.

[4] M. C. Vuran and I. F. Akyildiz, "XLP: A cross-layer protocol for efficient communication in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 11, pp. 1578–1591, Nov. 2010.

[5] O. Karaca and R. Sokullu, "Comparative study of cross layer frameworks for wireless sensor networks," in *Proc. 1st Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol. (Wireless VITAE)*, May 2009, pp. 896–900.

[6] K. Sharma and M. K. Ghose, "Cross layer security framework for wireless sensor networks," *Int. J. Secur. Appl.*, vol. 5, no. 1, pp. 39–52, 2011.

[7] T. Zia and A. Zomaya, "A security framework for wireless sensor networks," in *Proc. IEEE Sensors Appl. Symp.*, Feb. 2006, pp. 49–53.

[8] M. Xiao, X. Wang, and G. Yang, "Cross-layer design for the security of wireless sensor networks," in *Proc. IEEE 6th World Congr. Intell. Control Autom. (WCICA)*, vol. 1. Jun. 2006, pp. 104–108.

[9] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: Design considerations and research challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 2, pp. 107–130, 2015.

[10] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.

[11] I. F. Akyildiz, M. C. Vuran, and O. B. Akan, "A cross-layer protocol for wireless sensor networks," in *Proc. IEEE 40th Annu. Conf. Inf. Sci. Syst.*, Mar. 2006, pp. 1102–1107.

[12] H. Zhang and H. Shen, "Energy-efficient beaconless geographic routing in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 6, pp. 881–896, Jun. 2010.

[13] L. Galluccio, A. Leonardi, G. Morabito, and S. Palazzo, "A MAC/routing cross-layer approach to geographic forwarding in wireless sensor networks," *Ad Hoc Netw.*, vol. 5, no. 6, pp. 872–884, 2007.

[14] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, "SIGF: A family of configurable, secure routing protocols for wireless sensor networks," in *Proc. 4th ACM Workshop Secur. Ad Hoc Sensor Netw.*, 2006, pp. 35–48.

[15] Z. M. Hanapi, M. Ismail, K. Jumari, and M. Mahdavi, "Dynamic window secured implicit geographic forwarding routing for wireless sensor network," in *Proc. Int. Conf. Wireless Commun. Sensor Netw. World Acad. Sci., Eng. Technol.*, 2009, pp. 173–179.

[16] Z. M. Hanapi and M. Ismail, "Impact of blackhole and Sybil attacks on dynamic windows secured implicit geographic forwarding routing protocol," *IET Inf. Secur.*, vol. 8, no. 2, pp. 80–87, Mar. 2014.

[17] I. A. Umar, Z. M. Hanapi, A. Sali, and Z. A. Zulkarnain, "FuGeF: A resource bound secure forwarding protocol for wireless sensor networks," *Sensors*, vol. 16, no. 6, p. 943, 2016.

[18] D. Quercia, S. Hailes, and L. Capra, "B-trust: Bayesian trust framework for pervasive computing," in *Proc. Int. Conf. Trust Manage.*, 2006, pp. 298–312.

[19] M. Toulouse, B. Q. Minh, and P. Curtis, "A consensus based network intrusion detection system," in *Proc. IEEE 5th Int. Conf. IT Converg. Secur. (ICITCS)*, Aug. 2015, pp. 1–6.

[20] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4647–4658, Nov. 2014.

[21] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "E-hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 6, pp. 1156–1168, 2009.

[22] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw.*, 2005, pp. 1–10.

[23] T. K. Kim 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, 2008.

[24] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," *Comput. Netw.*, vol. 53, no. 14, pp. 2396–2407, 2009.

[25] A. Tajeddine, A. Kayssi, A. Chehab, and H. Artail, "Fuzzy reputation-based trust model," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 345–355, 2011.

[26] S. Renubala and K. S. Dhanalakshmi, "Trust based secure routing protocol using fuzzy logic in wireless sensor networks," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Dec. 2014, pp. 1–5.

[27] M. Zarei, A. M. Rahmani, A. Sasan, and M. Teshnehlab, "Fuzzy based trust estimation for congestion control in wireless sensor networks," in *Proc. IEEE Int. Conf. Intell. Netw. Collaborative Syst. (INCOS)*, Nov. 2009, pp. 233–236.

[28] P. Victor, C. Cornelis, and M. de Cock, "Trust and recommendations," in *Recommender systems handbook*. New York, NY, USA: Springer, 2011, pp. 645–675.

[29] 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.

[30] Z. Yao, D. Kim, and Y. Doh, "Plus: Parameterized and localized trust management scheme for sensor networks security," in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst. (MASS)*, Oct. 2006, pp. 437–446.

[31] J. Hur, Y. Lee, S.-M. Hong, and H. Yoon, "Trust management for resilient wireless sensor networks," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, 2005, pp. 56–68.

[32] R. Ferdous, V. Muthukkumarasamy, and A. Sattar, "Trust formalization in mobile ad-hoc networks," in *Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Apr. 2010, pp. 351–356.

[33] S. Tan, X. Li, and Q. Dong, "A trust management system for securing data plane of ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7579–7592, Sep. 2016.

IDRIS ABUBAKAR UMAR received the B.Eng. degree in computer engineering from Bayero University Kano, Nigeria, in 2008, and the M.Sc. in computer networks from University Putra Malaysia (UPM), in 2013. He is currently pursuing the Ph.D. degree with the Department of Wireless and Communication Networks, UPM. His research interests focus on protocol development, security, cloud computing, and Internet of things.

ZURINA MOHD HANAPI received the B.Sc. degree in computer and electronic system engineering from Strathclyde University in 1999, the M.Sc. degree in computer and communication systems engineering, University Putra Malaysia (UPM) in 2004, and the Ph.D. degree in electrical electronic, and system engineering from the Universiti Kebangsaan Malaysia in 2011. She is currently an Associate Professor with the Faculty of Computer Science and Information Technology, UPM, where she is also a Lecturer. She is also a Leader of some research projects and she has authored many conference and journal papers. Her research interests in routing, wireless sensor network, wireless communication, distributed computing, network security, cryptography, and intelligent systems. She received the Excellence Teaching Award in 2005, 2006, and 2012. She also received the Silver Medal in 2004 and the Bronze Medal in 2012.

A. SALI received the B.Eng. degree in electrical electronics engineering (communications) from The University of Edinburgh in 1999, the M.Sc. degree in communications and network engineering from Universiti Putra Malaysia (UPM) in 2002, and the Ph.D. degree in mobile satellite communications from the University of Surrey, U.K., in 2009. She was an Assistant Manager with Telekom Malaysia Bhd from 1999 to 2000. She was involved in EU-IST Satellite Network of Excellence (SatNEx) I and II from 2004 to 2009. She is currently an Associate Professor with the Department of Computer and Communication Systems, Faculty of Engineering, UPM, since 2003. She is also the Principle Investigator for projects under the funding bodies Malaysian Ministry of Science, Technology and Innovation, Research University Grant Scheme UPM and The Academy of Sciences for the Developing World Joint Grants. Her research interests are radio resource management, MAC layer protocols, satellite communications, wireless sensor networks, disaster management applications, 3-D video transmissions.

ZURIATI A. ZULKARNAIN received the Ph.D. degree from the University of Bradford, U.K. She is currently an Associate Professor with the Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM). She has served as a Head of Department of Communication Technology and Networks, Faculty of Computer Science and information Technology, UPM. She is currently is the Head of section for High Performance Computing for Institute of Mathematical Research, UPM. She is currently undertaking some National funded projects on QKD protocol for cloud environment and routing and load balancing in the wireless ad hoc network. She is also the Founder of ZA Quantum Sdn Bhd, a start-up company from UPM to produce a software designing tool for Quantum Communication known as quantum communication simulator. Her research interests include efficient multiparty QKD protocol for classical network and cloud, load balancing in the wireless ad hoc network, quantum processor unit for quantum computer, authentication time of the IEEE 802.15.4 with multiple key protocol, intra-domain mobility handling scheme for wireless networks, efficiency and fairness for new aimd algorithms and a kernel model to improve the computation speedup and workload performance. She has been actively involved as a member of the editorial board for some international peer-reviewed and cited journals.