Attack Resilient Trust and Signature-based Intrusion Detection Systems

Boniface Kabaso[1], Saber A. Aradeh[2], Ademola P. Abidoye[3]
Department of Information Technology, Cape Peninsula University of Technology
Cape Town, South Africa

***Abstract*—Wireless sensor networks have been widely applied in many areas due to their unique characteristics. These have exposed them to different types of active and passive attacks. In the literature, several solutions have been proposed to mitigate these attacks. Most of the proposed solutions are too complex to be implemented in wireless sensor networks considering the resource-constraint of sensor nodes. In this work, we proposed a hierarchical trust mechanism based on clustering approach to detect and prevent denial of service attacks in wireless sensor networks. The approach was validated through simulation using Network Simulator (NS2). The following metrics were used to evaluation the proposed scheme: packet delivery ratio, network lifetime, routing delay, overhead, and number of nodes. The proposed approach is capable of detecting compromised sensor nodes vulnerable to a denial of service attacks. Moreover, it is able to detect all sensed data that have been compromised during transmission to the base station. The results show that our method can effectively detect and defend against denial of service attacks in sensor wireless sensor networks.**

Keywords*—Wireless sensor network; routing attacks; public-key cryptography; packet dropping; denial of service attacks

I. Introduction

The self-organized Wireless Sensor Network (WSN) is used predominantly in tracking and monitoring applications, and it is made of battery-powered sensor nodes that communicate through a wireless medium [1]. WSNs are initially used in military operations for monitoring enemies' movements in a particular area. However, since the development of the Internet of Things (IoT), WSNs have been widely applied in many areas such as automobile industries, aviation, environmental monitoring, and many more areas [2]. The fast-growing sensor network has reached its presence in almost every sector replacing human intervention. The primary concerns of WSN are the utilization of sensor node resources, provision of security against malicious attacks, and the provision of efficient data delivery. The WSN adopts a clustering algorithm and routing protocol for avoiding the overutilization of the sensor node's resources. The clustering algorithm divides the nodes and performs routing activities based on the role of the cluster leader and members. It significantly reduces the energy consumption of each node. The routing protocols select a suitable path that does not impact the performance metrics of WSN and also provides energy efficiency. The routing protocols must be resistant to communication delay and packet losses. The function of sensor nodes is to sense, process, and transfer the data to the desired location while maintaining their reliability and confidentiality [3]. Both these parameters are affected due to the security threats in the networks. The resource vulnerabilities in the sensor network impact the design of effective security mechanisms. Several security mechanisms help in avoiding the attacks that target the routing functionality of sensor nodes.

A. The Conventional Security Mechanisms in WSN

One of the major concerns of security mechanisms in WSN is to provide secure transmission of data from the sender to the receiver end without much utilizing the sensor node resources. The security in traditional routing protocols placed in a dynamic environment is complicated, and communication is not adequately secured [4]. The design of security mechanisms must involve both proactive and reactive methodologies while protecting against attacks. When a malicious intruder attacks the network, the compromised nodes have to resist in a way that does not influence other legitimate nodes to fall for the attack. The difficult task of resisting the attack is to know the source of the adversary, and it can be done using Intrusion Detection Systems (IDS) [5]. Most of the security requirements are built on cryptographic schemes, IDS, and trust-based schemes. The trust-based mechanisms provide a secure transfer of data through trustworthy nodes in the network. The use of efficient cryptographic schemes along with robust intrusion detection systems can enhance security schemes [6]. Security management is also crucial for managing the security level and its energy consumption. The security mechanism introduced in the network must be compatible with all the components of the network otherwise it becomes the target for the attack [7]. Fig. 1 presents the types of conventional security mechanisms [8].

B. Rust-Based Management

Trust management is a required parameter in routing protocols and security mechanisms. It is used to determine whether a node is faithful enough to forward the data packets and store important keys [9]. It is used primarily to quantify the trustworthiness and reliability of individual nodes based on their behavior and past experiences [10]. A node is considered trustworthy depending on the packet forwarding rate, energy consumption, delay, and other factors depending on the application. The trust values must be accurately measured to provide reliable and robust security services the traditional trust management utilizes more energy and sensor node resources. The lightweight trust-based mechanisms need to be developed to overcome the issues of resource utilization and to provide efficient trust management. The trust-based management

scheme that helps in secure data transmission for WSN is presented in Fig. 2.

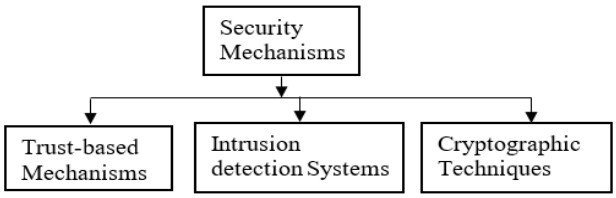

Fig. 1. The Conventional Security Mechanisms in WSN.

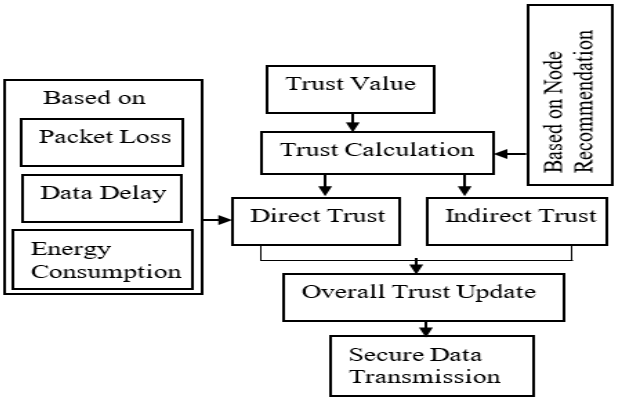

Fig. 2. Trust Management.

The trust-based mechanisms in WSN face some challenges during trust establishment [11]. Due to the storage and energy restriction in sensor nodes, the complexity of the trust value calculation must be less as possible. The validity of the trust value and the status of the node must neither be a long or short interval. The trust evidence has to be collected only during specific time intervals to avoid malicious attacks and wastage of energy resources. The level of trust requirements of the nodes must depend on the role it performs in the network. For example, the task of the cluster head is to carry all the essential information collected from the members to the base station, and hence the next-hop nodes of the cluster head through which it transmits the data to the destination must be more trustworthy.

Trust management schemes must be at least robust against the most common attacks as they will degrade the security requirements such as confidentiality and privacy of the network. The trust establishment process must occur in a secure channel as the integrity of the trust value is important to determine the node's honesty. The trust establishment methods must be flexible to dynamic topology networks and node behavior. As the location of nodes is hidden for security reasons in sensitive applications such as enemy monitoring in military applications, it is difficult to establish trust management mechanisms in an anonymous sensor network.

C. Hierarchical Routing Protocol

In the hierarchical routing protocols, the distribution of nodes is in the form of a tree-based structure, where nodes are assigned to perform specific roles based on the energy capability. For instance, the high-energy nodes are assigned important roles compared to low energy nodes [12]. The hierarchical routing protocol is more advantageous for real-time applications as it enhances the network lifetime by decreasing the transmission distance between the neighbor nodes used for transmitting the data to the destination. The hierarchical routing protocol can be cluster-based or chain-based. In cluster-based routing protocols, the nodes are classified based on energy capability as cluster heads and member nodes. The nodes with high energy are selected as cluster heads. The member nodes send the data to their respective cluster heads, and the cluster head then aggregates the information and forwards it to the base station.

D. Problem Statement

The routing protocols play a significant role in transferring the data packets to a destination in an efficient way, and data aggregation helps in reducing overall energy consumption and limited utilization of sensor node resources. In routing and data aggregation, the trustworthiness of nodes is a required parameter. Several trust-based schemes have been developed to achieve data forwarding by trustworthy nodes. In the traditional IDS schemes, the trust measurement is determined using a single metric, which in turn resulted in inaccurate detection. Thus, to overcome this issue, the use of multidimensional trust values such as Interactive Trust (IT), Honesty Trust (HT), and Content Trust (CT) is introduced during the trust calculation to improve the accuracy of the attack detection. IT is determined by the number of interactions between nodes in the network. The HT is determined based on the number of successful and unsuccessful interactions in the network while the CT is determined based on the capacity such as energy and the amount of data

E. Research Objectives

- To Develop and data delivery by energy-efficient security mechanism which provider trade o between utilization of sensor nodes.
- To evaluate the efficiency of the proposed scheme for achieving secure routing, the data packet dropping and modification attack model is designed.

F. Contributions

The contributions of this research are presented as follows:

1) The proposed contribution is built on an IDS model and is called IDS using Hierarchical Trust Measurement (IDSHT), where the trust measurement is done based on multidimensional factors such as IT, HT, and CT.

2) The signature-based mechanism is used for preventing common attacks, and the signature generation and verification are performed using the Rivest–Shamir–Adleman (RSA) algorithm.

II. Related Work

The energy-efficient routing protocols are surveyed mainly using three categories such as data-centric routing, hierarchical routing, and location-based routing. The location-based energy-aware reliable routing protocol (LEAR) [13] is a type of location-based routing protocol, which follows the

clustering algorithm. LEAR aims to reduce energy consumption by adopting geographical positioning and clustering technique. The routing table of each node is constructed using a distance of the neighboring nodes which in turn calculate the location information collected by Global Positioning Systems (GPS). When a node needs to send data, it refers to its routing table and thereby forwards the data to a neighboring node, which has the shortest distance. In [14], the authors proposed the Geographic and Energy Aware Routing protocol (GEAR) which deals with the use of geographic information while disseminating queries to required locations. The main idea of GEAR is to restrict the number of interests by sending interests to specific regions rather than the whole network. Each node in GEAR keeps an estimated cost and learning cost for reaching the destination through neighboring nodes.

Sensor Protocols for Information Via Negotiation scheme (SPIN) was proposed in [15]. It is a type of data-centric routing protocol which uses metadata negotiations to eliminate the transmission of redundant data throughout the network.

In [16] a systematic analysis of the threat posed by the Sybil attack in WSN is presented. The Sybil attack is defined as the malicious node legitimately taking on multiple identities of a node in the network. These attacks can affect the redundancy mechanism of the distributed data storage systems in peer to peer network. The authors highlight that the Sybil attack is a threat to essential functions such as routing, resource allocation, and misbehavior detection that can cause severe effects. The taxonomy of Sybil attacks is presented to understand and analyze the threat and its countermeasures in the network. The authors also discuss the different defense mechanisms against Sybil suited for WSN. The two methods presented are direct validation and indirect validation. The denial of service (DoS) attack is defined as any event that diminishes or eliminates network capacity to perform its expected function [17]. The different DoS attacks are jamming, collision attacks, unfairness attacks, black hole attacks, neglect and greed attack, homing attack, and misdirection attacks. The countermeasures for the jamming attack are by using spread spectrum, priority messages, and lower duty cycle.

The authors in [18] discussed the countermeasures taken against selective forwarding attacks. The analysis highlights that the security and on-time transmission of packets is the basic need for sensor network and the selective forwarding attacks targets these requirements.

The encryption schemes in WSN are categorized mainly into two types and they are symmetric key encryption schemes [19-22], and asymmetric key encryption schemes [23]. The authors in [24] introduced two building block security protocols such as SNEP (Secure Network Encryption Protocol) and Timed Efficient Streaming Loss-Tolerant Authentication TESLA. The SNEP protocol ensures data confidentiality, two-party authentication, and evidence of data freshness. The protocol is used to ensure authenticated broadcast for the resource constraint sensor network. Each node shares a secret key with the base station. During data communication, the two nodes consider an intermediate node such as a base station for setting a new key between them. The advantages of SPINS are resilient to node capture attacks, where any node does not leak any information about other sensor nodes, and it is easy to revoke key pairs in case of attacks.

In [25] the author proposed the Ambient Trust Sensor Routing (ATSR) protocol, which uses a trust management system for providing secure routing of data packets in the network. Each node in the network sends the periodic broadcast messages with node Identity (ID) and energy availability. A multicast message such as a reputation request message is sent periodically to the neighboring nodes for obtaining the indirect trust information, and the reply is gathered from unicast messages. The trust metrics used by nodes to evaluate the adjacent nodes are forwarding data rate, residual energy, and distance. The advantage of the ASTR scheme is that the data packets are forwarded based on the energy metric of the next-hop node thereby achieving energy conservation.

The authors in [26] presented a reputation-based event-triggered formation control (RETF) in which trust-related information about neighbor nodes is resolved and stored in the form of a set of modules by each node in the network. Several IDS mechanisms-based schemes have been introduced based on the types of attacks and application requirements to provide efficient detection of attacks before causing severe damage to the systems [27]. The authors presented an IDS survey based on the target WSN, detection technique, collection process, trust model, and analysis technique.

III. Framework for the Proposed Scheme

This section presents the framework for the proposed scheme based on based IDS-hierarchical trust (IDSHT) model. It adopts a cluster-based network using a two-tier hierarchical trust mechanism to reduce the energy consumption of the nodes in the system.

The nodes in the cluster-based network are classified into cluster head (CH), sensor nodes (SN), and base station (BS). In each cluster, the CH is selected based on the residual energy and transmission distance, and it forwards the data packets from the member nodes to the base station in an efficient manner the CH has more energy than the member nodes that communicate with their respective CH and have minimum energy. CH aggregates the data sent by the sensor nodes before sending it to the BS. The CH transmits the aggregated data to the base station directly. Each SN has a unique identity and belongs to a single cluster. The cluster head stores the data in the form of queues that are collected from the SN before forwarding it to the BS as shown in Fig. 3.

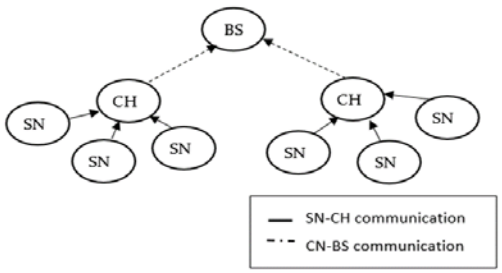

Fig. 3. Hierarchical Cluster-based Topology of Proposed IDSHT Scheme.

In the proposed scheme, each node in the network broadcasts the control information by attaching its ID and residual energy for identifying its neighbors. When the neighboring nodes receive the transmitted hello message, the neighbor nodes take the particular node as a neighbor and update the same in the adjacent table The conventional security mechanisms that are used for detecting attacks in the network have used only single metrics for evaluating trust in WSN. The main issue faced during the trust evaluation is the lack of accuracy in detection. The first level of trust in WSNs is the SN trust evaluation, which is done by CH in a particular cluster using the following multidimensional metrics discussed below.

1) Interactive Trust Evaluation of SNs (IT): The IT is calculated using the number of interactions of the SN in the network. The interactions of the SN include the sending and receiving data packets between the nodes and requests sent or forwarded from other nodes. The IT at the CH level is calculated using some interactions between CH and BS.

2) Content Trust Evaluation of SNs (CT): The CT is based on the trust evaluation of the observing data, and it is the data-centric trust evaluation calculated using a CH. The primary purpose of SNs is to sense the different parameters such as temperature, humidity, air pressure, and light intensity and transmit the observing data to the respective CHs.

3) Honesty Trust evaluation of SNs (HT): The HT is calculated using the number of successful and unsuccessful interactions between the CH and SN in the network. In HT, the CH overhears the SN when the interaction is unsuccessful. The trust evaluation at the CH level considers only the direct trust calculation using BS-CH evaluation. The trust evaluation in CH is similar to the SN level trust evaluation, and it includes multidimensional factors such as IT, CT, and HT. The IT, CT, and HT are calculated using the BS-CH evaluation while the CT includes the proximity of aggregated data and effective average observing data.

4) Content Trust Evaluation of CH (CT): The CT is de ned as the trust value obtained by the deviation between sensing data and an effective average of observed data. The CT of CH is calculated by BS according to the proximity of fusion data and effective average observing data of SN in the cluster. The overall trust of CH is calculated using BS by aggregating the multidimensional factors such as CTCH, HTCH, and ITCH evaluated for CH and is shown in equation 1. If the node launches the selfish attack, it will forward a false energy value in the control information to avoid being selected as a CH to preserve its energy.

$$OT_{ch} = W1 * IT_{ch} + W2 * HT_{ch} + W3 * CT_{ch} \quad (1)$$

where W_1=0.2, W_2 =0.4, W_3 =0.4.

Thus, the main issue faced with IDS schemes is that even after removing the malicious nodes, further attacks such as impersonation attacks are induced in the network. The impersonation attacks are serious attacks, where the adversary successfully uses one of the identities of legitimate nodes to provide a gateway for other types of attacks. The signature generation and verification using RSA algorithm security of the proposed IDSHT scheme can be improved by using signature generation, and verification mechanism, and it is termed as S-IDSHT. In S-IDSHT, each SN generates the public key and private key using the RSA algorithm. The SN forwards the data packet to their respective CHs after encrypting the data using the public key shared among the member nodes. After the data packet reaches the CH, the encrypted data is then decrypted using the private key, which is a secret key allocated for CH. Then, the CH aggregates all data along with the RSA signature collected from the member nodes and forwards it to the base station. The data aggregation during this process reduces the energy consumption of the overall network. The BS collects the data from all the CHs and decrypts the aggregated data using the unique private key and verifies the received data signature is the same as the original data. If the signature of the original data is not the same as that of the received data, then the node is said to be an adversary, and it is an impersonation attacker. If the signature of the original data is the same as the signature of receiving data, the node is said to be legitimate.

IV. Proposed Scheme Structure

The proposed IDSHT-S scheme adopts a hierarchical cluster-based structure to ensure secure and efficient data transmission during the routing and data aggregation process. The trust evaluation in the proposed scheme is based on the two-tier hierarchical trust mechanism, and the two levels of trust evaluation include the SN level and CH level. The trust value is calculated using multidimensional factors such as IT, CT, and HT. These multidimensional factors are used for finding the overall trust for SN and CH where the data is verified using signatures. The signature generation and verification in the proposed scheme are done using the RSA algorithm. SNs encrypt the data before transferring the data to the CH, which acts as an intermediate node and aggregator. The simulation scenario of the IDSHT-S scheme is constructed using the Network Simulator (NS2) tool. The proposed scheme is developed by modifying the Ad-hoc On-Demand Distance Vector (AODV) protocol files in NS2. In the experimental phase, the node formation is the first phase. After the selection of a source node and a destination node, the best path from the source to reach the destination is estimated by the AODV protocol. The AODV protocol is modified according to the application requirement. In the proposed scheme, the AODV protocol is modified the routing protocol based on IDSHT and IDSHT-S scheme objectives.

A. Hierarchical Trust Mechanism in IDSHT Scheme

One of the major concerns of security mechanisms in WSN is to provide secure transmission of data from the sender to the receiver end without much utilizing the sensor node resources. The security in traditional routing protocols placed in a dynamic environment is complicated, and communication is not adequately secured. In the proposed IDSHT scheme, the two-tier hierarchical mechanisms are introduced, and the trust evaluation for routing behavior and data aggregation is done using multidimensional metrics such as IT, T), and HT. The two levels of trust evaluation are done such as SN trust evaluation and CH trust evaluation. The first level of trust evaluation is simple, as the SN evaluation is done through

direct communication between CH and SN in a cluster. The second level consists of the trust evaluation at the cluster head level is explained along with its multidimensional factor evaluation.

B. Signature Based IDSHT Scheme

The main issue faced in IDS schemes is that even after removing the malicious nodes, further attacks such as impersonation attacks are induced in the network. The impersonation attacks are one of the serious attacks, where the adversary successfully uses one of the identities of legitimate nodes, and it uses these fake identities to provide a gateway for other types of attacks. The main aim of the impersonation attacks is to obtain confidential information that should be kept secret during the entire data transmission. Every node in the network encrypts its data and abstracts the information, which includes the data sending time, node ID, and ID of the data. After attaching the signature, the aggregated data is then sent to the BS. Through this method, the aggregated data can be verified by BS and confirm that every data forwarded to it is valid.

C. Signature Generation and Verification using RSA Algorithm

Signature generation and verification mechanisms are used as another security layer to improve the security of the proposed scheme. Thus, each SN generates the public key and private key using the RSA algorithm. The role of cryptographic techniques is to prevent any leakage or modification of confidential data in WSNs [28]. The leakage of data is prevented by encrypting the data using keys and sending the encrypted data to the destination. As most of the encryption and key management schemes require complex computation and increased costs, the need for designing lightweight cryptographic schemes and achieving a trade-off between providing security and limited utilization of resources has become a necessity [29]. The two types of cryptographic keys used for authentication and encryption are a public key and a private key. The public key is known by designated nodes, while private keys are kept secret by specific nodes. A digital signature is used for authentication and maintaining the message's integrity. The digital signature involves three algorithms such as key generation, signing, and signature verifying algorithm. The advantage of using a digital signature is that it is difficult to forge a user's signature without knowing the private key. Both IDS and trust-based schemes make sure that the attacks are not initiated in the network. The cryptographic schemes alone cannot provide an effective security mechanism, and it has to be combined with other security mechanisms to achieve all the security requirements of WSN. The data aggregation during this process reduces the energy consumption of the overall network. The BS collects the data from all the CHs and decrypts the aggregated data using the unique private key and verifies that the received data signature is the same as the original data. If the signature of the original data is not the same as that of the received data, then the node is said to be an adversary, and it is an impersonation attacker. If the signature of the original data is the same as the signature of receiving data, the node is said to be legitimate. In the proposed scheme, the data integrity and confidentiality of the data are secured, and efficient data transmission is achieved.

D. The Simulation Components for Network Scenario

NS2 Tool: The NS2 is an open-source event-driven simulator tool that is used in studying the dynamic nature of communication networks. The NS2 simulation tool is used for performing simulations in both the wired and wireless sensor networks.

C++: C++ is a high-level programming language used for graphical applications, and it is used in the back-end mechanism in NS2 tool. The C++ programming language is used for running the simulation, and all the C++ files are compiled and linked to create an executable file.

OTCL: The OTCL is a scripting language used for the configuration and setup of the simulation in NS2 tool. In NS2, the C++ objects are made available to the OTCL interpreter and can be controlled by OTCL level.

Network Animator (NAM) Output: The NAM is used to represent the network and packet traces graphically. It supports topology layouts, packet-level animation, and data inspection tools.

X-Graph: The X-graph program draws the graph on an X-display such that the data read from either data files or standard input if no files are displayed. The network scenario in the proposed IDSHT-S scheme is built in a hierarchical structure, and the cluster-based routing is used to provide efficient data transmission as shown in Fig. 4.

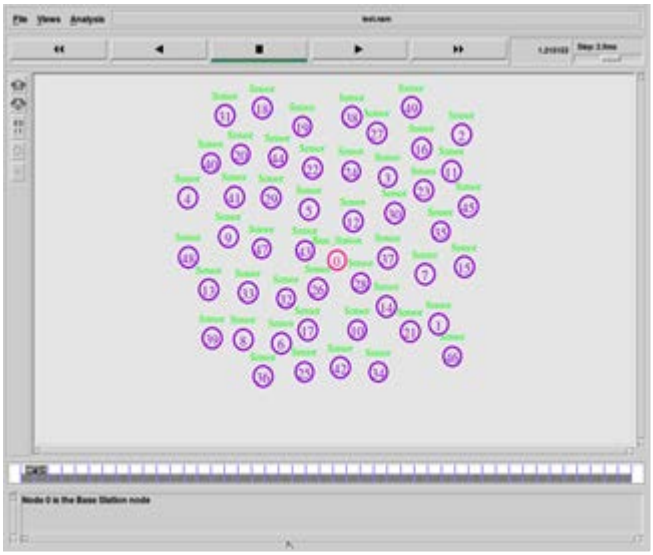

Fig. 4. The Network Scenario of the Proposed IDSHT-S Scheme.

V. Research Findings

Since there is a possibility to launch the impersonation attacks by the malicious nodes in WSN, the RSA is used for signature generation and verification processes. The proposed IDSHT-S modifies the AODV routing protocol files such as aodv.cc file concerning the proposed scheme. Comparison is made between the IDSHT-S and the existing IDSHT. Both are evaluated using the same simulation settings and compared to their outputs. The following metrics were used for the

evaluation: Packet Delivery Ratio (PDR), Network lifetime, Delay, and Overhead. The numbers of nodes are varied from 40 to 70 at 10 intervals each. Graphs are plotted for performance metrics using X-graph in NS-2.

1) Packet Delivery Ratio (PDR): The ratio between the total number of delivered packets to the base station and the total number of transmitted packets from the sensor nodes.

2) Network lifetime: The network lifetime represents the remaining energy of a node, which has minimum energy in the network.

3) Delay: Every node follows the secure routing protocol to deliver the data packets to the base station. Delay of a packet is defined as the average time taken by a node to deliver the data packets to the base station.

4) Overhead: The overhead is defined as the total number of control packets used in the network. The routing protocols exploit control packets to detect the routing paths to the base station. More control packets tend the sensors to spend a lot of energy and so maintaining the overhead while providing network security is essential.

5) Number of Nodes vs Packet Delivery Ratio: The packet delivery ratio depends on the number of data packets received at the base station and the number of packets forwarded by the CH after the aggregation process. The graph of the simulation result is drawn by plotting the number of nodes in the X-axis and packet delivery ratio on the Y-axis as shown in Fig. 5. The packet delivery ratio values are expressed in percentage for both the existing IDSHT scheme and the proposed IDSHT-S scheme.

6) Number of Nodes Vs Delay: The delay in WSN is the time taken by the data to reach the destination, i.e., base station. The delay of data packets affects the performance of the network. The delay in the system is mainly caused due to the dropping of the data packet. Node collision depends on the time taken for trust evaluation and other factors. The simulation graph for the delay is shown in Fig. 6 by taking the number of nodes on the X-axis and the delay expressed in seconds on the Y-axis.

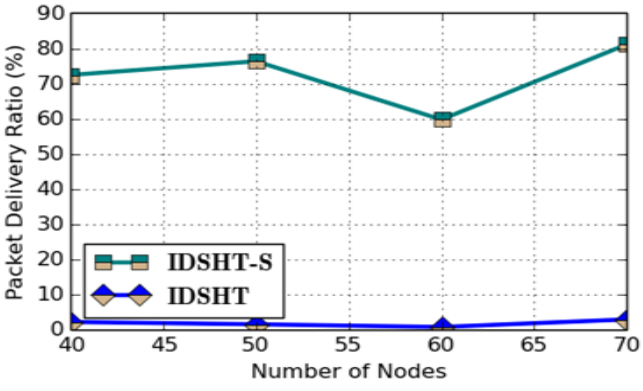

Fig. 5. The Simulation Graph for Number of Nodes vs Packet Delivery.

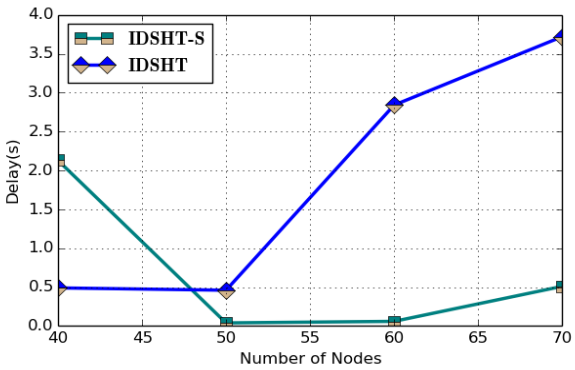

Fig. 6. The Simulation Graph for Number of Nodes vs Delay.

7) Number of Nodes vs Network Lifetime: The network lifetime is indirectly proportional to the energy consumption in the network. When energy consumption is large, the network lifetime is drastically reduced. The battery exhaustion in attacks occurs mainly due to malicious attackers and the proposed scheme aims at revoking these malicious attacks. The simulation results are presented in graphical form as shown in Fig. 7.

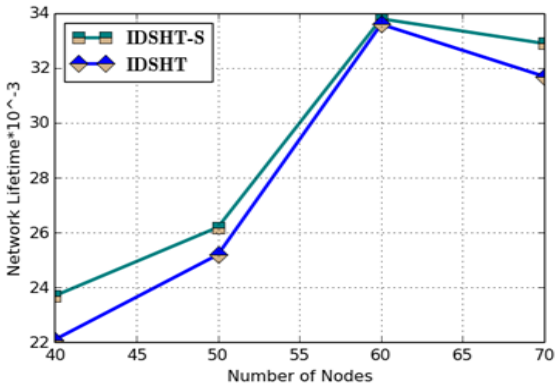

Fig. 7. The Simulation Graph for Number of Nodes vs Network Lifetime.

VI. Conclusion

Several trust-based security mechanisms have been developed to provide secure routing and data aggregation in WSN. The trade-off between energy efficiency and accurate trust calculation is one of the major concerns while developing intrusion detection schemes in WSN. In the proposed IDSHT scheme, a multi-dimensional two-tier hierarchical trust-based mechanism is adopted, which includes interactive trust, honesty trust, and content trust for cluster head selection during data aggregation. The IDHST scheme supports the WSN dynamic environment, transition state of nodes, and variation in trust values. IDHST includes both direct evaluations for trust calculation in a fixed hop range. The trust evaluation is maintained at two levels, where the multidimensional trust of the sensor node is maintained by the cluster head and the multidimensional trust of the cluster head is calculated from the base station and cluster head interaction, feedback evaluation from one-hop neighbors, and interactions with other cluster heads. The honesty trust is calculated using the number of successful and unsuccessful interactions between the two

nodes. The content trust is calculated based on the observing data by cluster heads and it is a network relates to trust. The interactive trust is evaluated by calculating the number of interactions between the nodes and cluster heads.

In future, we intend to implement the proposed scheme in a real test-bed.

VII. Future Work

In the future, we intend to implement all the algorithms in a real test-bed using the above metrics.

Declaration of Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

Authors' Contributions

All authors contributed and approved the final manuscript.

Data Availability

The raw data of the IoT devices used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] Y. Yuan, L. Huo, Z. Wang, and D. Hogrefe, "Secure APIT localization scheme against Sybil attacks in distributed wireless sensor networks," IEEE Access.vol. 6, pp. 27629-27636, 2018.

[2] R. Priyadarshi, B. Gupta, and A. Anurag, "Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues," The Journal of Supercomputing. pp. 1-41, 2020.

[3] Y.-G. Yue and P. He, "A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and future directions," Information Fusion.vol. 44, pp. 188-204, 2018.

[4] J. Tang, A. Liu, J. Zhang, N. N. Xiong, Z. Zeng, and T. Wang, "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," Sensors.vol. 18, no. 3, p 751, 2018.

[5] 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, 2019.

[6] A. G. Finogeev and A. A. Finogeev, "Information attacks and security in wireless sensor networks of industrial SCADA systems," Journal of Industrial Information Integration.vol. 5, pp. 6-16, 2017.

[7] M. Ge, K.-K. R. Choo, H. Wu, and Y. Yu, "Survey on key revocation mechanisms in wireless sensor networks," Journal of Network and Computer Applications.vol. 63, pp. 24-38, 2016.

[8] T. C. Jesus, P. Portugal, F. Vasques, and D. G. Costa, "Automated methodology for dependability evaluation of wireless visual sensor networks," Sensors.vol. 18, no. 8, p 2629, 2018.

[9] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," Transactions on Emerging Telecommunications Technologies.vol. 26, no. 2, pp. 107-130, 2015.

[10] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An efficient dynamic trust evaluation model for wireless sensor networks," Journal of Sensors.vol. 2017, 2017.

[11] S. Sharma and S. K. Jena, "Cluster based multipath routing protocol for wireless sensor networks," ACM SIGCOMM Computer Communication Review.vol. 45, no. 2, pp. 14-20, 2015.

[12] X. Liu, "Atypical hierarchical routing protocols for wireless sensor networks: A review," IEEE Sensors Journal.vol. 15, no. 10, pp. 5372-5383, 2015.

[13] R. Alasem, A. Reda, and M. Mansour, "Location based energy-efficient reliable routing protocol for wireless sensor networks," Recent Researches in Communications, Automation, Signal processing, Nanotechnology, Astronomy and Nuclear Physics, WSEAS Press, Cambridge, UK. pp. 180-185, 2011.

[14] S. Roychowdhury and C. Patra, "Geographic adaptive fidelity and geographic energy aware routing in ad hoc routing," in: Proceedings - international conference, 1, pp. 309-313, 2010.

[15] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks," Wireless Networks.vol. 8, pp. 169 – 185, 2002.

[16] N. Alsaedi, F. Hashim, A. Sali, and F. Z. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)," Computer communications.vol. 110, pp. 75-82, 2017.

[17] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," IEEE Access.vol. 6, pp. 6975-7004, 2018.

[18] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," IEEE Transactions on Wireless Communications.vol. 15, no. 5, pp. 3718-3731, 2016.

[19] P. Sinha, V. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," in: Proceedings - 2017 International Conference on Signal Processing and Communication (ICSPC), pp. 288-293, 2017.

[20] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications.vol. 36, no. 1, pp. 16-24, 2013.

[21] I. S. Gawdan and Q. I. Sarhan, "Performance Evaluation of Novel Secure Key Management Scheme over BAN Wireless Sensor Networks," Journal of University of Duhok.vol. 19, no. 1, pp. 179-188, 2016.

[22] A. Khan, S. W. Shah, A. Ali, and R. Ullah, "Secret key encryption model for Wireless Sensor Networks," in: Proceedings - 2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 809-815, 2017.

[23] D. H. Kurniawan and R. Munir, "Double Chaining Algorithm: A secure symmetric-key encryption algorithm," in: Proceedings - 2016 International Conference On Advanced Informatics: Concepts, Theory And Application (ICAICTA), pp. 1-6, 2016.

[24] B. Mbarek and A. Meddeb, "Energy efficient security protocols for wireless sensor networks: SPINS vs TinySec," in: Proceedings - 2016 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-4, 2016.

[25] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," Wireless personal communications.vol. 69, no. 2, pp. 805-826, 2013.

[26] F. M. Zegers, M. T. Hale, J. M. Shea, and W. E. Dixon, "Reputation-Based Event-Triggered Formation Control and Leader Tracking with Resilience to Byzantine Adversaries," in: Proceedings - 2020 American Control Conference (ACC), pp. 761-766, 2020.

[27] R. Mitchell and R. Chen, "A survey of intrusion detection in wireless network applications," Computer Communications.vol. 42, pp. 1-23, 2014.

[28] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "Detecting data semantic: a data leakage prevention approach," in: Proceedings - 2015 IEEE Trustcom/BigDataSE/ISPA, 1, pp. 910-917, 2015.

[29] H. Tawalbeh, S. Hashish, L. Tawalbeh, and A. Aldairi, "Security in Wireless Sensor Networks Using Lightweight Cryptography," Journal of Information Assurance & Security.vol. 12, no. 4, 2017.