A Novel Energy-efficient Wormhole Attack Prevention Protocol for WSN based on Trust and Reputation Factors

Saad Al-Ahmadi
Department of Computer Science, King Saud University, Riyadh, Saudi Arabia

Keywords: Network Security, Trust Mechanism, Wireless Sensor Networks, Wormhole Attack, WSN Simulation.

Abstract: The deployment of Wireless Sensor Networks (WSNs) for the Internet of Things (IoT) is important, but this also poses some security issues. Wireless Sensor Networks (WSNs) are vulnerable to various attacks, such as the Wormhole attack. The Wormhole attack is one of the most severe attacks on WSNs that is particularly challenging to defend against even when the communication is authentic, and sensors are not compromised. Existing techniques to detect and protect against Wormhole attacks place a substantial burden on the scarce sensor resources and do not consider the dynamic nature of the network. In this paper, a novel Energy Efficient Wormhole Attack Prevention Protocol (EWATR) is proposed to protect WSNs against Wormhole attacks. EWATR is based on trust and reputation among WSN nodes that consider the dynamic nature of the network. This study also compares EWATR against several state-of-the-art trust and reputation models through extensive simulations using the TRMSim-WSN simulator. Eventually, the simulation results show the superiority of EWATR over other proposed protocols in terms of efficient energy consumption and shorter path length.

1 INTRODUCTION

Wireless Sensor Networks (WSNs) consist of large numbers of low-power sensors dynamically forming different topologies. WSNs are notable for their distributed cooperation, dynamic topology, lack of central administration, open medium, and constrained capability (computation and power constraints). Every sensor serves as both a host and a router, forwarding packets to and from other sensors. Sensors have many limitations that require keeping in mind while establishing networks, like limited memory size, battery life, and processing performance (Akyildiz et al., 2002). WSN is vital for the Internet of Things (IoT) and has numerous military applications, environment monitoring, predictive maintenance, smart grids, transportation, buildings, healthcare, to name a few (Agrawal et al., 2011).

WSN Security is a significant concern because sensors interact with their surroundings and people are often physically accessible, allowing possible physical attacks. WSNs are more vulnerable than traditional wired and wireless networks to security threats. A wormhole attack is a severe threat where powerful routers are injected in strategic locations to tunnel packets received in one network and replay them in another place. The attacker only needs two transceivers and no key material.

There are many solutions proposed in the literature to protect WSN against wormhole attacks. This paper presents a novel Energy Efficient Wormhole Attack Prevention Protocol (EWATR) based on trust and reputation among WSN nodes to combat wormhole attacks. It uses cooperation to establish trust among neighbouring sensors. EWATR can be embedded in nay WSN routing protocol, such as Ad hoc On-Demand Distance Vector (AODV), to detect and prevent wormhole attacks. It can be extended to other ad hoc networks such as the Wireless Ad-hoc network (WANET), where route discovery and node credibility are the first security requirements in wireless routing protocols.

This paper is arranged as follows: Section 2 introduces the reader to the necessary background information. In contrast, Section 3 covers an extensive literature review of the state-of-the-art research for detecting and preventing wormhole attacks— Section 4 presents the proposed approach EWATR. In Section 5, we show our comparison results using simulation versus other existing techniques. Section 6 concludes the work and sheds light on future work.

Al-Ahmadi, S.
A Novel Energy-efficient Wormhole Attack Prevention Protocol for WSN based on Trust and Reputation Factors.
DOI: 10.5220/0010951400003118
In *Proceedings of the 11th International Conference on Sensor Networks (SENSORNETS 2022)*, pages 191-201
ISBN: 978-989-758-551-7; ISSN: 2184-4380

2 BACKGROUND

A wormhole attack is a severe WSN attack in which the attacker fakes two sensors as the wormhole tunnel ends, one of which collects, captures the packets, and forwards them through the tunnel to the other. By enabling smoother transmission channels, the tunnel allures adjacent nodes to direct their traffic via the tunnel rather than different safe routes. When wormhole nodes only forward packets faster, it is considered a passive attack. When a wormhole alters packet content or drops them, it is regarded as an active attack. As a Denial-of-Service attack, the wormhole distorts data aggregation and routing protocols.

Therefore, the attacker can initialize the wormhole using malicious nodes deployed in several locations to capture network traffic (packets or bits). It redirects the network packets using inside an extended distance tunnel. The wormhole tunnel was established using either a wired link or high-frequency wireless links (Aliady & Al-Ahmadi, 2019).

Figure 1 shows communication between the source node S and the base station. The safe path, shown in dotted lines, is long and has many hops, while the dangerous path, shown in dark thick lines, has fewer hops and passes through a wormhole tunnel between the two malicious nodes W1 and W2 (Chiu & Lui, 2006). In some cases, the tunnel establishes a shortcut route that makes the tunnelled packet arrives with fewer hops and shorter time. The confidentiality and authenticity of the communication channel do not defend against such a dangerous attack (Ban et al., 2011).

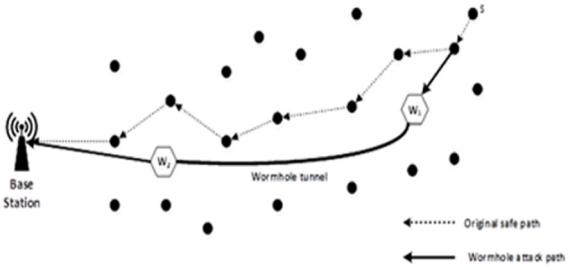

Figure 1: Wormhole attack.

2.1 Wormhole Attack Classification

Wormholes are classified into three types: closed, half-open, and open (N. Sharma & Singh, 2014), as shown in Figure 2. Nodes S and D are the source and destination nodes. Nodes M1 and M2 represent the malicious nodes. Nodes A, B are benign nodes on the route between S and D. Curly braces "{}" are used to hide nodes invisible nodes to S and D. because they are in the wormhole. The word "closed" means "start from and include," while the word "open" means "start from but not include" (N. Sharma & Singh, 2014).

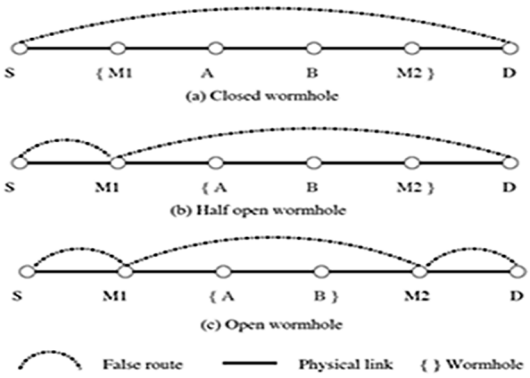

Figure 2: Types of Wormhole attack.

In closed wormhole attack (a), M1 and M2 take over the neighbourhood discovery beacons between S and D, where they assume they are direct neighbours to each other while they are not. In half-open wormhole attack (b), M1 is a neighbour of S and tunnels beacons through M2 to D. Only one malicious node is visible to S and D. Similar situation can happen to D where it can see a neighbouring wormhole node M2 and tunnels beacons through M1 to S. In the open mode wormhole (c), both wormholes M1 and M2 are visible direct neighbours to S and D.

2.2 Wormhole Attack Modes

Wormhole attacks are classified according to techniques used to establish the attack, such as encapsulation, out-of-band channel, packet relay, protocol deviation, and high-power transmission. Packet encapsulation is considered an easy way to launch a wormhole attack. There is no need for extra specialized hardware or tools, and each packet is routed only via the legitimate path. This attack class is based on freezing the hop counter by encapsulating the packets that reached the wormhole ends. The packet is transported into the original form by the second endpoint (Ghugar & Pradhan, 2019). Therefore, this prevents the right functional nodes from finding the shortest paths between them and generates many fake neighbours since the hop counter is unrealistic.

Using Out-of-Band mode needs much effort to lunch since it needs extra hardware. It relies on hardware rather than software. This mode is deployed

with at least two malicious nodes equipped with a long-range directional wireless link or a direct wired link (Ghugar & Pradhan, 2019).

Packet relay mode can be deployed with at least one malicious node without specialized hardware by initializing a fake neighbour relation between two right functional indirect nodes and fabricating a neighbour relation. The malicious node tunnels packets between indirect nodes, thus controlling all the traffic without changing the routing protocol.

Protocol deviation attacks can cause serious harm to the ad hoc network and WSN (Padmavathi & Shanmugapriya, 2009). It acts as a massive Denial of Service (DoS) attack. This attack is also known as the Rushing Attack. It is launched against many existing on-demand routing protocols by using one or more malicious nodes. In many existing routing protocols such as AODV and DSR, a node can discover the destination route by sending multiple RREQ packets to know the suitable route to the destination node. Each node forwards the RREQ packet only once to prevent this flood's high overhead. The intruder will abuse this property in this attack by forwarding the RREQ route discovery packet to other nodes. It will cause any node to receive the rushed RREQ will discard any further RREQ from the same route discovery.

The high-power transmission attack's main idea is to use a high-power source such as an electromagnetic radio frequency signal to send a high-power broadcast to various network nodes. Therefore, nodes that received the transmitted high-power broadcast rebroadcast it to the destination node. This method deploys the wormhole tunnel simply without using any colluding node. Also, malicious nodes are on the route between the source and the destination nodes (Johnson et al., n.d.).

2.3 Countermeasures to Wormhole Attacks

This section will briefly describe other detection and prevention techniques of wormhole attacks in WSN proposed by several researchers.

2.3.1 Secure Geographic Routing Protocol

Detecting wormholes based on a node's geographical location is a typical detection and prevention technique—the coordinates of every node within the WSN are used for secure geographic routing. The sender node includes its current geographical location in the packet and the time stamp so the receiver node can verify communication and falsify malicious nodes. The receiver node calculates the possible and estimated transmission range and checks the eligibility of transmission time. This technique requires an accurate and synchronized timer with a geographic positioning system such as GPS to obtain good results. The usage of additional hardware has many disadvantages, such as exceeding the overall network cost and reducing battery life, especially within the WSN that uses small or low power sensors. There are many existing geographic protocols, for example, Greedy Perimeter Stateless Routing (GPSR) (Ratnasamy et al., 2001). GPSR is inspired by a greedy algorithm where every node within the network knows its current location by using beacons to identify the closest neighbour and near the ultimate destination.

2.3.2 Statistical Analysis Approach

One possible solution to detect and forestall the wormhole attack is using statistics and probabilities. We can utilize this vital information to see the wormhole tunnel by studying nodes' routes, frequency, and neighbour discovery. The statistical analysis approach can provide the right solution depending on the sensors and network configuration. For example, if the sensors have a set of radio frequency ranges within fixed boundaries, detecting the malicious node that uses a high-power transmission would be more straightforward and notable. The researchers proposed a new statistical analysis scheme that explores the network routes by a statistical routing protocol (Somu & Mallapur, 2019). It can spot the attack by inspecting the behaviour of the sensors and the transmitted information. Other researchers have suggested statistical techniques that focus intensely on investigating the state of sensor nodes and their closest neighbours. Based on the received neighbourhood information, the base station(s) can discover the presence of wormholes probabilistically using hypothesis testing (Buttyán et al., 2005).

2.3.3 Cryptography Key

Using public or symmetric key cryptography is a method proposed by many researchers. Keys building and exchange techniques for secure transmission in distributed environments is a challenging task. Encryption and decryption in WSN consume large amounts of those limited sensor resources such as processing capabilities, memory available, and little energy (Babaeer & Al-Ahmadi, 2020). In (Zhang et al., 2006), a new scheme based on public and private authentication keys was proposed to eliminate

malicious nodes before packet sending. The researchers have suggested a key management scheme based on the public key exchanging methods to improve security matters in ad hoc networks and WSNs (Salam et al., 2010). In (Ju, 2012), Elliptic Curve Cryptography (ECC) is used as a routing-driven key management scheme to help the exchange mechanism between neighboring nodes. Nodes only accept packets from authenticated neighbors with a valid key and ignore other packets coming from fake nodes. In this way, malicious nodes cannot connect with rightful nodes to gain trust and validity. Another critical management scheme solution was proposed in (P. Sharma, 2012), where three keys were used for different purposes. A global key (network key) is generated periodically by the base station. All nodes share it in the network and are used to encrypt all broadcasted messages within the network. The last two keys are pair-wise keys used by network nodes for authentication and exchanging secure messages purposes. An asymmetric cryptography-based key management scheme was suggested in (Khalil et al., 2007). It adopts a new fundamental management approach by inheriting the advantages of asymmetric cryptography and employs it efficiently for delivering session keys to sensor nodes.

2.3.4 Trust Mechanism

Trusted-based is another approach that has been proposed by many researchers as a solution to wormhole attacks as well as other attacks like sink-hole attacks, black hole attacks, and DoS attacks. The trust is built in the network layer routing protocol by building trusted links among all nodes within the WSN before establishing communication. In (Simaremare et al., 2013), the researchers have proposed a model improving security in ad hoc On-Demand Distance Vector (AODV) routing protocol by adding a trust factor that consists of three primary agents: trust agent, reputation agent, and combined agent. The trust agent model records the node's trust information so the reputation agent can spread the recorded data to all nodes. The combiner agent generates consolidated trust factors from the previous agents' received information. Based on AODV, a local and global trust calculation method is proposed in (P. Sharma, 2012) to detect and prevent ad hoc network attacks. The Trust AODV (TAODV) calculates trust by gathering all activity information from surrounding nodes. It enhances the existing AODV by introducing new fields into the node's routing table to record other nodes' positive and negative feedback. A node is known for its trustworthiness if the input from other nodes is positive. Opinions among nodes change dynamically with the rise of successful or failed communication times. The AODV routing protocol is subject to extensive research and has many variations, yet it is still an open research area because of its flexibility.

3 LITERATURE REVIEW

The wormhole attack problem got the attention of many researchers because it is a crucial issue in WSN and it affects routing protocols and network lifetime. In the literature, many wormholes detection approaches have been proposed. The authors proposed a robust trust model for a cluster-based network in (Gautam & Kumar, 2018) to secure against collusion attacks. The model is based on direct trust using a time-lapse function. The function takes advantage of the forgetting curve to calculate direct trust—another reputation function used for indirect trust (recommendation-based trust) calculation. The cluster head plays the recommendation manager's role and builds indirect trust by collecting information from all neighbours of the target node. Simple mathematical operations calculate direct trust, and it entirely depends upon the packet transaction among nodes. Active and trust communication among nodes is achieved when the trust value is high. This model does not provide complete trust information because it only considers communication trust.

A MANET is a decentralized, ordinary, and self-orbiting type of wireless network that has the capability of managing mobile nodes. To detect wormhole attacks in MANET, a lightweight approach has been proposed in (Zardari et al., 2018). All replies (RREP) packets with sequence numbers are stored temporarily at the source node. The source node calculates an average of all sequence number and then store it. If any of the nodes exceeds the average, it will discard all replies packets. Hence, wormhole nodes can be eliminated from the network, and those nodes will be communicating in the network who are trusted. The proposed approach in this study is power-efficient, less complex, and increases network lifetime in large networks.

A similar task has been done in (An & Cho, 2021) to detect wormhole attacks in WSN. When events occur in the WSN, the sensor node in the vicinity of the generation event recognizes the event, generates a report of the detected event, and sends it to the base station. A wormhole attack, where in the report is sent over a various path than the original path, can happen

during the transmission process. As a result, a wormhole attack is detected, including encrypted node ID and hop count into the report content during the statistical en-route filtering methods report production process. Furthermore, in this study, they proposed a wormhole detection technique that can enhance security. The proposed approach detects both wormhole attacks and false report injection together.

Ukil in (Ukil, 2010) presents a simple yet efficient model based on collaborative computing through trust and reputation. It gives the possibility to find an optimal routing path that optimizes both reliability and communication efficiency. In the case of a trusted environment, no authentication is needed for a node to communicate with other nodes and to unwrap hidden keys. Reputation is a global phenomenon that tends to the history of the trustworthiness of nodes. The proposed model gives reliability preference over efficiency to protect and secure the network from insider threats. A worm propagation detection scheme was presented in (Ho & Wright, 2017), according to which a randomized-SPRT (Sequential Probability Ratio Test) was built on sequential traffic analysis to detect worm propagation through legitimate traffic. Detector nodes observe communication patterns in the network and identify the worm propagation pattern. After the initial remote attestations to detect infected nodes, detector nodes create chains of connections that would not be seen in regular traffic due to its spreading hop-by-hop. When some nodes are compromised, a self-propagating malicious code can take over the network and cause damage. The authors presented a methodology based on round trip time (RTT) and hop count to identify wormhole attacks (M. A. Patel & Patel, 2018). This approach requires two steps; the first step uses a hop counting mechanism based on the RTT algorithm. In every sensor node, built local maps to detect abnormalities and use a diameter feature transmission range. In the second step, both neighbours' ids and RTT are collected between every two successive nodes. This technique does not need any specialized hardware and saves energy consumption. Simulation results show that this scheme has high detection accuracy.

The study (N. Sharma et al., 2020) proposes a technique in which each node's trust value is calculated by watching N2N packet delay during packet transaction between neighbouring nodes, and malicious node identification is conducted based on this trust value. The trust value can also be used to choose a secure way and make a routing decision. For network performance valuation, the DSR routing protocol is utilized in the existing malicious nodes.

The researchers produced a defence method to protect wormhole attacks using the neighbour information collected for all nodes in WSN (Chu et al., 2019). This mechanism does not require extra hardware, complex calculation and does not consume significant resources. The proposed method depends on a Quantum-inspired Tabu Search (QTS) algorithm. This algorithm relies on finding combinations of the nodes to indicate the detection of wormholes. The experimental results show that the detection of wormhole attacks is highly successful.

A similar situation appears in ad hoc network, Mobile ad-hoc networks (MANETs), needs protection from various attacks like the wormhole that benefits from the absence of centralized infrastructure. In MANETs, routing suffers when a participating node does not set its intended function and performs malicious activity. The attacker can record packets at one location in the network, transfer them to another location, and retransmits them into the networks. Researchers introduced a modified AODV to discover wormhole attacks without specialized hardware such as a directional antenna and a specific synchronized clock (Gupta et al., 2011). Their protocol is independent of the physical medium of the wireless network. In route discovery, the source node starts the wormhole detection process in the discovered path, which counts hop difference among the neighbours of one of the hops away nodes. The destination node discovers a wormhole if the hop difference between neighbours of the nodes exceeds the acceptable level. The algorithm uses an additional hound packet to check if the ad hoc network is formed between trusted parties. It does not require sending a hound packet when the network is public, or nodes experience a high packet dropping rate. The hound packet is sent after the path discovery phase. The simulation results show that the algorithm works well in detecting wormholes of extensive tunnel lengths.

The researchers introduced Multi-Layered Intrusion Detection (MLDW) as a method for detecting and preventing wormhole attacks on MANET in (C.P & Saviour Devaraj, 2013). MLDW utilizes the AODV route discovery phase with adequate response time and uses layer framework information such as link latency estimator, intermediate neighbour node discovery mechanism, packet drop calculator, and node energy degrade estimator followed by isolation technique. MLDW does not require any specialized hardware or clock synchronization and achieves good defence results.

Authors in (M. Patel et al., 2019) have presented various detection features that help for wormhole detection. Existing wormhole detection techniques

mainly rely on four detection features: time, neighbourhood, location, and hop count. The time feature indicates that the suspicious path has more average time per hop than the safe path. Techniques based on time information require clock synchronization—the neighbourhood feature used by detection techniques to store information on one hop or two hops' neighbours. Analysing and storing two hops neighbour's data in the network requires more storage processing, power, and memory. The location feature is significant for detecting wormhole to know the location need to direct antennas and GPS. The hop count feature shows that wormhole attracts traffic by advertising a shorter route with a fewer hop count—existing techniques used hop count feature in collaboration with location and time features.

The authors proposed a new method for preventing wormhole attacks by using an algorithm to manage many nodes using node ID (Buch & Jinwala, 2011). In this method, Node ID was linked to the surrounding nodes in a binary tree structure. The algorithm created a load balancing feature for monitoring a hierarchical system for nodes and an extra packet header on each node to ensure it was not compromised. The experiment developed a simulation using C# on the Windows platform to study only the binary structure of how the nodes severed in a mesh network.

A Wormhole Resistant Hybrid Technique (WRHT) was presented as a more positive way of detecting the presence of a wormhole attack than existing strategies in (Singh et al., 2016). WRHT relies on the concept of watchdog and Delphi schemes and verifies that the wormhole will not be left untreated in the sensor network. WRHT depends on the dual wormhole detection mechanism of calculating probability factor time delay and packet loss probability of the established path to find the value of wormhole presence probability. All nodes in the path are given a different ranking and, subsequently, colours according to their behaviour. It does not require additional hardware such as a global positioning system (GPS), timing information, synchronized clocks, or high computational needs like traditional cryptographic schemes. The experimental results showed significant improvement in the detection rate of the wormhole attack.

4 PROPOSED APPROACH

The proposed protocol is an Energy Efficient Worm-hole Attack prevention scheme in WSN based on Trust and Reputation factor (EWATR). It makes use of trust and reputation information (Khalid et al., 2013) to calculate the trustworthiness of a node to judge a node's misbehaviour and effectively distinguish between normal operating and malicious nodes. In EWATR, the positive and negative effects of a node's action are observed. The observations are aggregated in a specific trust table maintained by the node. Statistical analysis is performed on the trust table data to generate the node reputation.

Node's trust computation based on:

- information collection,
- information dissemination,
- information mapping to trust model, and
- Decision making.

4.1 Information Collection

Information is collected by node (say A) through packet broadcasting. Node A monitors another node (say B) in promiscuous mode. When node B takes the responsibility to forward the packet received from A, it will broadcast it so node A can hear it again. Now, node A will verify the packet contents and update the trust rating for node B. In this manner, nodes can collect what is called *first-hand* trust information. When a sensor node broadcasts a packet, the node monitors the neighbouring node through a watchdog mechanism. After sending the packet to a neighbour, the watchdog mechanism requires that the node monitor the neighbour in a promiscuous mode, as illustrated in figure 3, to verify whether the neighbour has forwarded or intentionally dropped the packet. If the neighbouring node takes the packet forwards, the trust rating is incremented and updated in the sender nodes database. Conversely, if the adjacent node drops the packet, the trust rating is reduced in the sender node's database.

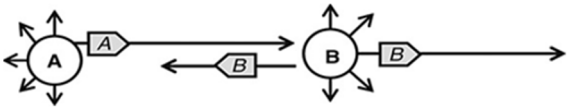

Figure 3: Description of promiscuous mode.

4.2 Information Dissemination

In EWATR, network nodes distribute their *first-hand* information to the neighbouring nodes. Such kind of distribution information is called *second-hand* information, as implemented in Figure 4. The use of *second-hand* information is beneficial and makes the reinforcement of the reputation process faster. *Second-hand* information sets up a global view of trust in the network. The nodes extend *second-hand* information either proactively, after some fixed time,

or reactively, on the occurrence of some event or some essential change in the network.

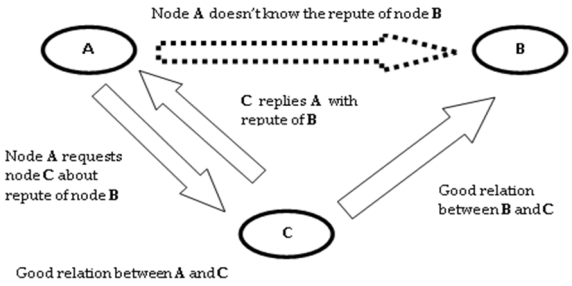

Figure 4: Second-hand trust information dissemination.

4.3 Information Mapping to the Trust Model

In this phase, network nodes add first-hand and second-hand information to produce a trust and reputation metric. First-hand data is direct, and more computation effort is required to combine first-hand data into the reputation metric. The credibility of the reporting node is made through various techniques suggested in the literature. One such technique, called the deviation test, is presented in (Ganeriwal et al., 2008). The following inequality represents the deviation test: Where d is a threshold, the value of which is set truly. In the inequality given in Equation (1), α and β are two parameters of the statistical Beta distribution, which is used for decision-making.

$$\left| \left(Beta(\propto,\beta)\right) - E\left(Beta\left(\propto_f,\beta_f\right)\right)\right| \geq d \qquad (1)$$

Here, α select right nodes while β selects nodes with bad behaviours. The probability value E (Beta(α, β)) is the measure of the current trust information node A has about node B, whereas E (Beta(αf, βf)) shows the new trust information provided by some node C to node A about node B. The reporting node C is considered trustworthy if the left-hand side of the difference in Equation (1) produces a value less than threshold d.

Various trust and reputation mechanisms use different statistical models to estimate the correctness of second-hand information, relying on the application and security requirements. The most used schema is the Beta distribution, whose probability density function is expressed using the Gamma function as

$$P(x) = Beta\ (\propto,\beta) = \frac{\Gamma(a,\beta)}{\Gamma(a)\Gamma(\beta)} x^{a-1}(1-x)^{\beta-1}, \forall 0 \leq x \geq 1, \propto \geq 0, \beta \geq 0 \qquad (2)$$

Where α refers to the acceptable behaviour, and β represents the bad behaviour of a node. Equation (2) suggested another way of measuring the consistency of data by a reporting node. For example, let us assume a node B provides trust information to node A for P+Q times. If information is regular for p times, then P(x) is implemented to predict its regularity in the subsequent observation. If P(x) results in a value equal to 1, then the reported information is regular and authentic; otherwise, it is considered unauthentic information.

4.4 Decision Making

The final step shows the decision-making process. The decision relies on the computed trust values. Node A decision may be one of the two binary values, where a "1" refers to participating and forwarding the packet, and a "0" means not cooperating. Figure 5 graphically illustrates the decision-making process.

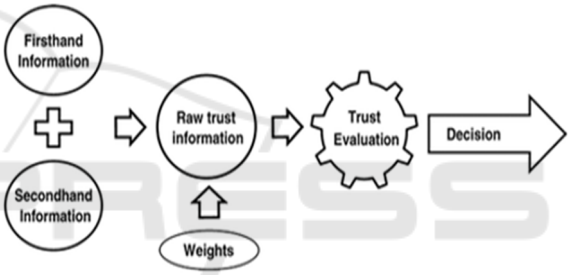

Figure 5: Trust computation process shows how weights applied to set trust thresholds.

5 EXPERIMENT EVALUATION

We simulated three experiments to evaluate and compare the performance of BTRM-WSN (Gómez Mármol & Martínez Pérez, 2011), Eigen Trust (Kamvar et al., n.d.), Peer Trust (Xiong & Liu, 2004), Power Trust (Zhou & Hwang, 2007), Linguistic Fuzzy Trust Model (LFTM) (Mármol et al., 2010), and Trust and Reputation Infrastructure Based Proposal model (TRIP) (Mármol & Pérez, 2012). The first experiment runs on comparing the seven systems in terms of accuracy in searching for trustworthy sensors. This experiment estimates the level of security provided in WSN. The second experiment compares the average path length leading to the trustworthy sensors selected. It assesses the efficiency, or the facility for discovering reliable sensors, of the seven techniques. Finally, the total energy saving of applying these seven techniques in WSNs is measured. The average Path length is the

efficiency measurements in ease of discovering sensor nodes.

5.1 TRMSim-WSN Simulation

We implemented the seven trust and reputation model simulators for WSN using TRMSim-WSN (Mármol & Pérez, 2009). It is a java-based trust and reputation model simulator that provides a straightforward method to test a trust and reputation model over WSN and compare it against other models. TRMSim-WSN users may choose between static and dynamic networks, as well as the proportion of fraudulent nodes, the percentage of nodes functioning as clients or servers, etc. We set up WSN based on network parameter settings shown in table 1. In a randomly created WSN, 30% of all nodes are clients that will request default services. The other 70% nodes will be servers, which are asked to provide services upon request. WORMHOLE NODES act in pairs for a single transaction when two legitimate nodes are supposed to communicate (for sharing of files between two legitimate nodes). There may be more than two nodes, both even or odd nodes. Statistical analysis may give more accurate results (Johnson et al., n.d.). If the movements are random in the network, wormhole nodes may have trouble catching up dynamically. Similarly, it is hard for legitimate ones to detect untrustworthy nodes.

Furthermore, in a typical transaction, two WORMHOLE nodes are needed for the tunnel to be established; one may be a Server node, while the one at the other end will be a client sensor node.

Having 70 percent server nodes and 30 percent client nodes means there are more sensing nodes information being transmitted by servers than by clients, which means that a client may be sending requests to more than one server node, at a time. A broadcast message by the client may reach multiple Server or even client nodes. Interestingly, a wormhole may also send a broadcast to the serving node and its other peer (worm) closest to the client node.

In network topologies in an infrastructure-based client-server model, clients are more than a single Server. For instance, a Webserver may serve thousands of clients' requests a second.

This may be because sensing information like humidity, temperature, wind speed, etc. maybe being more often transmitted to hub/gateway/hybrid nodes, which in turn may transmit or relay to infrastructure nodes.

Table 1: Experiment Parameters.

NumExecutions	100	%Clients	20%
NumNetworks	100	%Relay	5%
MinNumSensors	{50,100,150,200}	%Malicious	70%
MaxNumSensors	{50,100,150,200}	Radio range	{10, 8, 6, 4}

5.2 Accuracy

To estimate the reliability and level of security provided by the trust and reputation system in WSN. The accuracy of a trust and reputation system is implemented by the percentage of times when it successfully selects trustworthy sensors (the former situation) out of the total number of transactions.

When a transaction take place, it from wormholes. It may take several rounds of transactions, after which the culprit nodes are caught.

Figure. 6 demonstrates the accuracy of BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM, TRIP, and EWATR Techniques with various sensor nodes over WSN. We conclude that the EWATR technique can approximately provide the highest accuracy and, consequently, the highest level of reliability and security, while TRIP offers the lowest value. Furthermore, it has been observed that the Peer Trust model is the most oscillated and unstable accuracy. Fig 6 shows accuracy calculations based on static WSN. For nodes with similar movements, it may be difficult for wormhole nodes to catch up to locked-in victim nodes in all the above-mentioned techniques. Hence repeating the exercise for movements based on WSN may be futile.

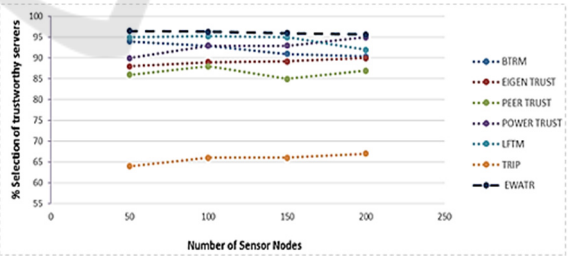

Figure 6: Selection percentage of trustworthy servers over static WSNs.

5.3 Path Length

The path length is the rate hops that lead to the most trustworthy sensors selected by the client in a WSN using a particular trust and reputation system. It assumed that less average path length indicates better performance in efficiency and facility searching for

trustworthy sensors of a trust and reputation system. The reasons behind this claim: 1) fewer intermediaries mean higher security level; and less energy consumption; and 2) shorter path length refers to that it is easier to find honest nodes, and thus, server nodes will respond quicker to client nodes.

Figure 7 compares BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM, TRIP, and EWATR in terms of rate path length leading to trustworthy sensors with various sensor nodes over WSN. TRIP and EWATR have the highest performance since, in TRIP, the rate path length remains one by increasing the number of sensor nodes. Moreover, Eigen Trust has the lowest performance in terms of shorting average path length. Eigen Trust, Power Trust, and Peer Trust are unstable and lengthiest in average path length that BTRM, LFTM, TRIP, and EWATR models.

With TRIP, the number of the hop, i.e., average distance, remains the same, i.e., one. This means that the Client and Server nodes are adjacent. The Wormholes attack strives on spoofing and fooling the Server-Client, that the best path between these is through these.

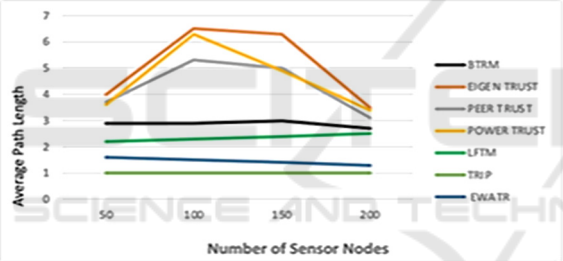

Figure 7: Average path-length leading to trustworthy servers over static WSNs.

5.4 Energy Consumption

Energy consumption of the network is the overall energy consumed in (1) client nodes sending request messages; (2) server nodes sending response services; (3) energy consumed by malicious nodes which provide inadequate services; (4) relay nodes that do not provide services; and (5) the energy to execute the trustworthy sensor searching process of a particular trust and reputation system. How to effectively reduce energy consumption is the main problem in WSN research. Wormholes increase the wireless energy transmission to fake being closer to sensor nodes and thus gain trust and access to genuine nodes. This also fakes path lengths. It takes several rounds to detect culprit nodes, by which time, critical battery drainage may have occurred in some cases. In some instances, mini solar panels are utilized in WSN, which only get a few minutes of light, e.g., in the canopy of forests.

Figure 8 compares the energy consumption of BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM, TRIP, and EWATR, respectively, over WSN and by various sensor nodes. It can be concluded that EWATR is the most energy consumption model in WSN environments, while TRIP is the least energy consumption.

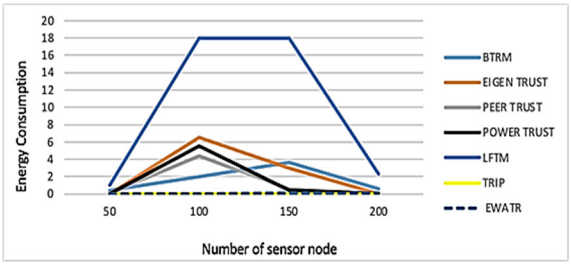

Figure 8: Network energy consumption over WSNs.

6 CONCLUSIONS

The wormhole attack employs various modes to launch one of the most severe malicious threats to WSN. Self-configuring and autonomous systems, such as WSNs, rely on trust to make successful judgments upon recognizing a misbehaving node. The task of building trust and reputation becomes challenging when the nodes are mobile. We have suggested the EWATR protocol and compared it with BTRM-WSN, Eigen-Trust, Peer-Trust, Power-Trust, LFTM, and TRIP. This paper concluded that the EWATR technique's accuracy approximately provides the best accuracy and, thus, the best level of reliability and security. While rate path length concludes, TRIP and EWATR have the highest performance, and Eigen Trust has the lowest performance in terms of shorting rate path length. Also, the energy consumed conducted that EWATR is the most energy consumption model in WSN environments, while TRIP is the least energy consumption. Future work will evaluate the proposed algorithm for various network conditions, such as frequent link breaks between nodes, which is a typical problem in a practical setting.

REFERENCES

Agrawal, S., Jain, S., & Sharma, S. (2011). A survey of routing attacks and security measures in mobile ad-hoc networks. *ArXiv Preprint ArXiv:1105.5623*.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer Networks*, *38*(4), 393–422.

Aliady, W. A., & Al-Ahmadi, S. A. (2019). Energy preserving secure measure against wormhole attack in wireless sensor networks. *IEEE Access*, *7*, 84132–84141. https://doi.org/10.1109/ACCESS.2019.2924283

An, G. H., & Cho, T. H. (2021). Wormhole detection using encrypted node IDs and hop counts in the event report of statistical en-route filtering. *International Journal of Computer Networks and Applications*, *8*(4), 390–399. https://doi.org/10.22247/ijcna/2021/209705

Babaeer, H. A., & Al-Ahmadi, S. A. (2020). Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking. *IEEE Access*, *8*, 92098–92109. https://doi.org/10.1109/ACCESS.2020.2994587

Ban, X., Sarkar, R., & Gao, J. (2011). Local connectivity tests to identify wormholes in wireless networks. *Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 1–11.

Buch, D., & Jinwala, D. (2011). Prevention of Wormhole Attack in Wireless Sensor Network. *International Journal of Network Security & Its Applications*, *3*(5), 85–98. https://doi.org/10.5121/ijnsa.2011.3507

Buttyán, L., Dóra, L., & Vajda, I. (2005). Statistical wormhole detection in sensor networks. *European Workshop on Security in Ad-Hoc and Sensor Networks*, 128–141.

Chiu, H. S., & Lui, K.-S. (2006). DelPHI: wormhole detection mechanism for ad hoc wireless networks. *2006 1st International Symposium on Wireless Pervasive Computing*, 6-pp.

Chu, T.-H., Kuo, S.-Y., & Chou, Y.-H. (2019). Using Quantum-inspired Tabu Search Algorithm with Logic Operation and Moving Average Indicator for Wormhole Attack Detection in a WSN. *Journal of Internet Technology*, *20*(1), 167–176.

C.P, V., & Saviour Devaraj, A. F. (2013). MLDW- A MultiLayered Detection mechanism for Wormhole attack in AODV based MANET. *International Journal of Security, Privacy and Trust Management*, *2*(3), 29–41. https://doi.org/10.5121/ijsptm.2013.2303

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *4*(3), 1–37.

Gautam, A. K., & Kumar, R. (2018). A robust trust model for wireless sensor networks. *2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 1–5.

Ghugar, U., & Pradhan, J. (2019). A Review on Wormhole Attacks in Wireless Sensor Networks Intrusion detection of various attack in WSN View project A Review on Wormhole Attacks in Wireless Sensor Networks. *International Journal of Information Communication Technology and Digital Convergence*, *4*(1), 32–45. https://www.researchgate.net/publication/336798552

Gómez Mármol, F., & Martínez Pérez, G. (2011). Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication Systems*, *46*(2), 163–180. https://doi.org/10.1007/s11235-010-9281-7

Gupta, S., Kar, S., & Dharmaraja, S. (2011). WHOP: Wormhole attack detection protocol using hound packet. *2011 International Conference on Innovations in Information Technology*, 226–231.

Ho, J. W., & Wright, M. (2017). Distributed detection of sensor worms using sequential analysis and remote software attestations. *IEEE Access*, *5*, 680–695. https://doi.org/10.1109/ACCESS.2017.2648853

Johnson, M. O., Siddiqui, A., & Karami, A. (n.d.). *A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks*.

Ju, S. (2012). A lightweight key establishment in wireless sensor network based on elliptic curve cryptography. *2012 IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment*, 138–141.

Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (n.d.). *The EigenTrust Algorithm for Reputation Management in P2P Networks*.

Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., Kolodziej, J., Wang, L., Zeadally, S., & Chen, D. (2013). Comparative study of trust and reputation systems for wireless sensor networks. *Security and Communication Networks*, *6*(6), 669–688.

Khalil, I., Bagchi, S., & Shroff, N. B. (2007). Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Computer Networks*, *51*(13), 3750–3772.

Mármol, F. G., Marín-Blázquez, J. G., & Pérez, G. M. (2010). Linguistic fuzzy logic enhancement of a trust mechanism for distributed networks. *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*, 838–845. https://doi.org/10.1109/CIT.2010.158

Mármol, F. G., & Pérez, G. M. (2009). TRMSim-WSN, trust and reputation models simulator for wireless sensor networks. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2009.5199545

Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, *35*(3), 934–941.

Padmavathi, G., & Shanmugapriya, M. D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. In *IJCSIS) International Journal of Computer Science and Information Security* (Vol. 4, Issue 1).

Patel, M. A., & Patel, M. M. (2018). Wormhole attack detection in wireless sensor network. *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, 269–274.

Patel, M., Aggarwal, A., & Chaubey, N. (2019). Analysis of Wormhole Detection Features in Wireless Sensor Networks. *International Conference on Internet of Things and Connected Technologies*, 22–29.

Ratnasamy, S., Francis, P., Handley, M., Karp, R., & Shenker, S. (2001). *A Scalable Content-Addressable Network*.

Salam, M. I., Kumar, P., & Lee, H. (2010). An efficient key pre-distribution scheme for wireless sensor network using public key cryptography. *The 6th International Conference on Networked Computing and Advanced Information Management*, 402–407.

Sharma, N., Sharma, M., & Sharma, D. P. (2020). A Trust based Scheme for Spotting Malicious Node of Wormhole in Dynamic Source Routing Protocol. *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 1232–1237.

Sharma, N., & Singh, U. (2014). Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks. *International Journal of Computer Science and Mobile Computing*, *3*(2), 29–33.

Sharma, P. (2012). Trust based secure AODV in MANET. *Journal of Global Research in Computer Science*, *3*(6), 107–114.

Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. (2013). Secure AODV routing protocol based on trust mechanism. In *Wireless Networks and Security* (pp. 81–105). Springer.

Singh, R., Singh, J., & Singh, R. (2016). WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks. *Mobile Information Systems*, *2016*. https://doi.org/10.1155/2016/8354930

Somu, P., & Mallapur, D. (2019). Research Trends in Secure Routing Protocols and Communication System in WSNs. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 3413–3421.

Ukil, A. (2010). Trust and reputation based collaborating computing in wireless sensor networks. *2010 Second International Conference on Computational Intelligence, Modelling and Simulation*, 464–469.

Xiong, L., & Liu, L. (2004). Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, *16*(7), 843–857.

Zardari, Z., Memon, K., Shah, R., Dehraj, S., & Ahmed, I. (2018). A lightweight technique for detection and prevention of wormhole attack in MANET. *ICST Transactions on Scalable Information Systems*, 165515. https://doi.org/10.4108/eai.13-7-2018.165515

Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). Location-based compromise-tolerant security mechanisms for wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 247–260.

Zhou, R., & Hwang, K. (2007). Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Transactions on Parallel and Distributed Systems*, *18*(4), 460–473.