Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.025752
Article

Modified Adhoc On-Demand Distance Vector for Trust Evaluation And Attack Detection

S. Soundararajan[1,*], B. R. Tapas Bapu[2], C. Kotteeswaran[1], S. Venkatasubramanian[3], P. J. Sathish Kumar[4] and Ahmed Mudassar Ali[2]

[1]Anna University, Chennai, 600025, Tamil Nadu, India
[2]S.A. Engineering College, Veeraraghavap, Chennai, 600077, Tamil Nadu, India
[3]Saranathan College of Engineering, Trichy, 620019, Tamil Nadu, India
[4]Panimalar Engineering College, Chennai, 600069, Tamilnadu, India
*Corresponding Author: S. Soundararajan. Email: Soundararajanphd1@yahoo.com
Received: 03 December 2021; Accepted: 04 March 2022

Abstract: Recently, Wireless Sensor Network (WSN) becomes most potential technologies for providing improved services to several data gathering and tracking applications. Because of the wireless medium, multi-hop communication, absence of physical protectivity, and accumulated traffic, WSN is highly vulnerable to security concerns. Therefore, this study explores a specific type of DoS attack identified as a selective forwarding attack where the misbehaving node in the network drops packet on a selective basis. It is challenging to determine if packet loss is caused by a collision in the medium access path, poor channel quality, or a selective forwarding assault. Identifying misbehaving nodes at the earliest opportunity is an acceptable solution for performing secure routing in such networks. As a result, in this study effort, we present a unique Modified Ad Hoc On-Demand Distance Vector (AODV) Routing protocol depending upon the One time password (OTP) method that employs the RSA algorithm. Finally, a trust evaluation process determines which approach is the most optimal. According to the simulation findings of the suggested routing protocol and comparison with existing routing protocols provided in this article, the proposed work is both efficient and cost-effective.

Keywords: Wireless sensor network; selective forward attack; one time password; trust evaluation; RSA algorithm

1 Introduction

Because of the rising needs in electronics and computer technologies, the spread of Wireless Sensor Network (WSNs) has developed as a promising new development [1]. In general, the construction of a WSN comprises numerous ultra-compact independent devices, known as sensor nodes that are dispersed over a specified region [2]. A sensor node is a battery-operated device that is integrated to sensors, processor, transceivers [3], and is powered by batteries. The ability to execute mission-critical activities in unattended and even hostile situations, such as battle field reconnaissance and homeland security

surveillance, is enabled by this [4]. The sensor devices' energy, processing, and communication capabilities must be restricted in order for the sensor nodes to be economically viable [5]. Aside from that, sensor nodes are frequently placed in easily accessible locations, increasing the likelihood of a physical attack [6].

During data transmission, the sensor nodes included in WSNs are subject to network assaults, which compromise the nodes and cause them to become inoperable [7]. Data aggregation is carried out in order to minimise the quantity of data transmitted by removing redundant data [8]. Consequently, in large-scale WSN, sensor nodes closer to one other frequently have overlapping sensing ranges and so detect the same phenomena, resulting in the generation of enormous amounts of duplicate data [9]. Sensing networks are thus faced with whole new difficulties, which cannot be addressed directly by using the same old security approaches that have been employed in traditional networks in the past [10]. Because of this, secure data aggregation methods must be built such that they can continue to function effectively without being compromised even in the midst of network assaults [11]. The provision of security in WSN is particularly difficult because of the resource constraints of sensor nodes [12], as previously stated.

In WSN, when every individual sensor node is composed of a sluggish, low powered CPU with just 4 KB of RAM space [13], asymmetric cryptosystems are not viable to employ. In order to do this, symmetric key algorithms are used in the designing of key management protocols for WSN [14]. In order to utilise key management protocol depending upon the symmetric shared keys, it is necessary to solve a number of basic issues, one of which is the methods that are used to primarily create the shared keys. Using protocols like as TLS and Kerberos, which were originally designed for wired networks but are now unfeasible to utilize in large-scale WSN due to the restricted energy, processing, and communication abilities of the sensors.

In the past, researchers concentrated their attention to monitor the loss of packets in each communication and separating the nodes with high packet loss from data forwarding channel. The data delivery ratio and network performance can be improved with these methods, but they have minimal influence to identify the selective forwarding assaults. Here, the hostile node will transmit the control packets as usual while intentionally dropping data packets from the network. In general, the selective forwarding attacks corrupt the data transmission for sensitive and non-sensitive based environments. These attacks damage the whole environment and thus the malicious nodes must be predicted for avoiding the sensitive packets dropping. In something like a selective forwarding attack (SFA) [14], the adversary, acting as a normal node in the routing process, excludes messages from surrounding nodes. Non-critical data may be transmitted regularly, but significant information, such as notifications prompted by an adversary in a practical weapon, may be ignored [15]. When sensitive data is compromised, the assault has the potential to do significant harm because the primary issue in attack detection is distinguishing between malicious and regular packet losses, the normal packet loss should be taken into account while evaluating forwarding. Further, the nodes which are selectively dropping the packets are hard to determine in the sparse environment since it seems like the normal nodes [16,17]. To overcome the research issues of the existing approaches, this paper has some contributions that are follows:

- To identify selective forward attacks in the network, we have developed a unique OTP-based trust mechanism
- Presenting the integration of a multi-level authentication system with the trust mechanism, which ensures the maximum security for users

The structure of the study is given here: Section 2 summarizes some of the most current research in the field of WSN attack detection. Section 3 provides an overview of the detection technique that will be used in the proposed study. After providing an overview of the proposed work's simulation findings in Section 4, and Section 5 draws the conclusion.

2 Related Works

Some of the very recent works related to the proposed work is listed as follows:-looked into a particular type of Denial of Service (DoS) attack in Wireless Mesh Network (WMN), they discovered that it was known as elective forwarding attack. An attacker can trick a malfunctioning mesh router into only forwarding a part of the receiving packets, while dropping the rest of them. Many research works have concentrated on the selective forwarding attacks with the consideration of the ideal wireless channels; however, they took into account an increasingly realistic and difficult situation where packets are dropped as a result of an attack or as a result of normal loss event like medium access collisions or poor channel quality, respectively. In particular, they created a channel aware detection (CAD) method that is capable of distinguishing between selective forwarding misbehaviour and regular channel losses. The channel estimate strategy and the traffic monitoring strategy were both used in the development of the CAD algorithm. It was determined that the observed loss rate at a particular hop exceeded the anticipated typical loss rate, and the nodes involved were labelled as "assailants".

Authors concentrated their attention on a specific form of DoS attack known as elective forwarding or grey-hole attacks. If the attacks get conducted at the gateway of the WMN, it has the potential to cause serious harm as a result of the loss of confidential information. This work suggested a forwarding assessment based detection (FADE) technique for reducing collaborative Grey hole attack. FADE, in particular, identifies complex assaults through the use of forwarding evaluations that are helped by two-hop acknowledgement monitoring, among other techniques. Furthermore, FADE may coexist with modern link security methods without causing conflict. They investigated the best detection threshold which reduces the total of the False Positive Rate (FPR) and False Negative Rate (FNR) of the proposed technique while taking into account network dynamics produced by decreased channel quality or medium access collision, among other things. For solving the problem of the detection of selective forwarding attack, the development of a trust model was undertaken. (1) Local and global attack detection via mutual monitoring among all nodes is the primary goal in the proposed method to system maintenance, and (2) recognition of aberrant driving pattern by malevolent nodes are the secondary goals in the proposed approach to system maintenance. Because the technique made use of in-band as well as out-of-band data, it was successful in low-density road circumstances and robust to a variety of situations, like varying rates of malicious occurrences or road ranges. According to the results of the comprehensive simulations, the technique accomplished an improved fault tolerance by selecting the trustworthy nodes for data transmission and identifying the malicious nodes with a reasonably maximum degree of accuracy.

Authors proposed a new energy efficient selective forwarding attack detection technique. The method keeps track of the whole network based on the time taken for a packet to travel down a route to reach its destination. The routes that have the possibility to include attack nodes were subjected to the lazy detection technique. The suggested approach can reduce the cost of detecting selective forwarding attacks to a minimum as a result of this. For examining the supremacy of the presented technique, the researchers undergone a comparison study with the already available schemes. Overall, the method achieves a detection rate that is comparable to the previous scheme while reducing needless data transfers by about 35.7% when compared to the existing scheme.

Authors have focused on Selective forwarding attack, which a harmful attack exists in the WSN. Several defence mechanisms are developed for addressing the elective forwarding attack. The authors have discussed the available defence approaches available in the literature along with their limitations and thereby provide a brief overview of the present solution space. The authors have also categorized the reviewed approaches based on the characteristics and defence scheme.

3 Modified Aodv Based Selective Forward Attack Detection in WSN

WSNs are typically placed in open regions that are also unstable, as is the case with most urban areas. A collision between a wireless channel and a medium access point might result in significant regular packet losses. Since, it will be vulnerable for different routing protocol attacks, comprising particular forwarding, black hole and wormhole attacks, among others. In a straightforward type of selective forwarding attack, hostile node attempts to halt the flow of packets over the network by declining forwarding data or dropping the data that pass via their network interface. The selective forwarding attacks were disguised by the regular packet loss, making it more difficult to detect the assaults. It is complicated to identify and mitigate selective forwarding attacks while simultaneously improving network speed.

With this highly flexible network, the AODV protocol is proposed, however it only saves the shortest path to the destination. When a link fails, it must rediscover the route, which adds to network congestion. In this research, we develop the traditional AODV routing mechanism and present MAODV, a newly developed AODV routing protocol that considers route reliability in order to construct a more reliable path from source to destination. We made an adjustment to the Hello and RREQ message formats in MAODV to capture the transmission time and route stability factor, respectively. The Modified AODV (MAODV) routing protocol based on the OTP-based RSA algorithm and Trust Evaluation, is designed to discriminate between normal packet loss and Selective Forward Attack when data forwarding. Therefore, it is needed to derive a network model to demonstrate the relevance of the proposed research effort, which is discussed in further detail in the next sections.

3.1 Assumptions and System Model

3.1.1 Network Model

Consider that a WSN has comprised of collection of arbitrarily dispersed sensor node, represented by N, and a sink node that is responsible for monitoring an open space. A communication protocol used by sensor nodes to interact with its surrounding nodes is the IEEE 802.11 DCF. Aggregation points can provide nodes with routing information, and nodes can put their faith in the fact that messages delivered to aggregation points will be correctly mixed with other messages and sent to a base station. The behaviour of any node is represented using a random variable F(s), which is distributed according to the Bernoulli distribution principle, which is given by:

$$F(s) = \begin{cases} 1, & s \text{ forwards the packet} \\ 0, & s \text{ drops the packet} \end{cases} \tag{1}$$

To construct the route between the source to the destination, each node requires to broadcast the continuous hello messages to identify the connectivity. Here the hello message format is modified than the traditional AODV routing protocol and the sending time, a new field that added to the packet format and the new format for packet header is follows,

$$< \text{Dest\_Addr},\ \text{dest\_Sequence\_id},\ \text{Hop Count},\ \text{Lifetime},\ \text{and Send Time} >$$

The nodes in the network observe the packet forwarding nature for every single hop neighbouring node using the promiscuous learning. All the nodes are homogenous in nature with respect to energy, queue sizes, computation, and interface.

3.1.2 Threat Model

Sensor nodes that have been compromised can conduct selective forwarding attacks to impair network performance. If a hacked node gets a data packet, it maliciously declines it with a probability known as attack probability. Because the hacker may manipulate the attack probability of compromised nodes, determining

whether packet loss resulted from the varying channel conditions or intentional drop is challenging, particularly for nodes with minimal attack probability.

3.1.3 Assumptions

Prior to the procedure of placing the node in the network, the key server creates a pair of unique one-time passwords (and), one of which is a prime integer. The unique OTP is communicated by the sensors and base station (BS), and it may be utilized for data encryption at the node. At the time of deployment, it is assumed that the sensors could obtain its location details and roughly synchronise its time with the BS. Furthermore, the attacker fails to compromise a node at the time of brief deployment period. To avoid attracting suspicion, malicious nodes selectively drop a tiny fraction of all passing packets; that is, they do not drop all packets.

3.2 Modified AODV (MAODV) Routing with OTP employed RSA Algorithm

In the same way that existing AODV routing protocols build routes only when they are required, the proposed routing protocol employs the same principle. The system makes use of standard routing table with one entry per destination, and sequence number to identify the updated routing data and avoid routing loop. In AODV routing, a set of control messages are involved namely routing request message (RREQ), which is advertised by node to other nodes in the need of a route, routing reply message (RREP), which is unicast back to source of the RREQ, and route error message (RERR), which is broadcasted to inform other nodes regarding the loss of connection. HELLO messages are also utilized to other purposes, such as identifying and monitoring connections with nearby neighbours. The suggested routing protocol is a kind of modified AODV routing protocol, which is based on the RSA algorithm, as described above. Flowchart depicting the MAODV routing protocol's process flow is given in Fig. 1.

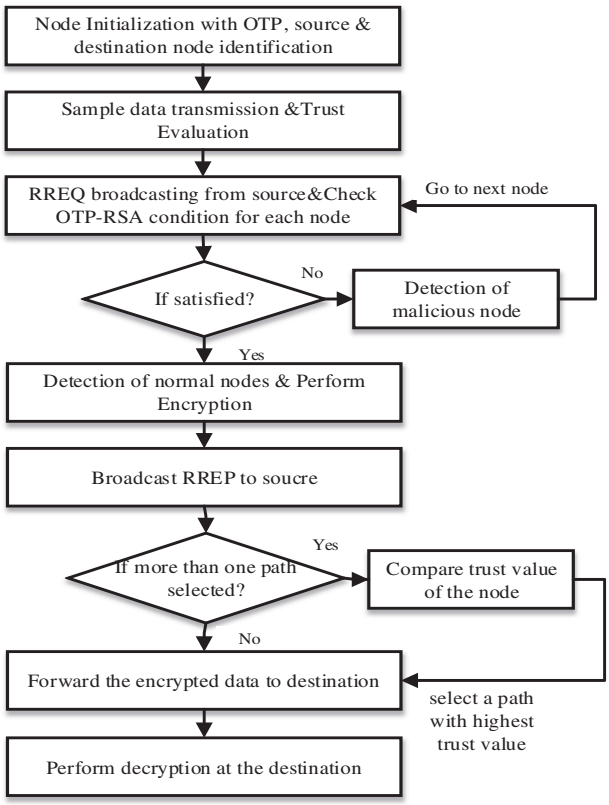

Figure 1: Process flow of the proposed work

The MAODV routing protocol is partitioned into setup, route discovery, and route maintenance phases. The MAODV routing protocol features a setup phase that is quite similar to the conventional AODV routing protocol in terms of functionality. At the second phase, the innovative aspects of the proposed routing protocol first appear. The source node broadcasted an RREQ packet to all of its neighbour nodes to identify the best path in the network. The packet is sent via the neighbouring nodes until it reaches the target node, at which point it is dropped. The proposed routing system is reactive in nature, and it begins by forwarding a sample packet across the nodes to demonstrate its functionality. Using the trust value of the nodes after a sample packet transmission, the malicious nodes in the network may be recognized and eliminated from further consideration.

3.2.1 Trust Evaluation

The trust estimation component assesses the trustworthiness of neighbours by listening in on their transmissions in promiscuous mode and dynamically identifying misbehaving nodes. Based on the observed data, the trust model categorizes all monitored sensor nodes into one of three categories: trustworthy node, malicious node, or defective node. Assume that nodes I j, and s are neighbours and engage in packet forwarding amongst a pair of source and destination nodes. If node I and node s discover a match in matching items, node j is deemed a trustworthy node. When the packet ID in the overheard packet from node j are much lesser than those in the buffer, but the packet hash values match the buffer content, node I and node s classify node j as defective. If the node j sends a fake response representing correct packet forwarding to node s but drop each received packet from node I it may misinform node I but not node s, because node s is notice malicious behaviour by relating equivalent entries in buffer with packet ID and hash values in overheard packets.

The node i and node s recognize true behaviour of node j by detect and aggregate amount of packet forwarding performance of node j. Let $T_{i,j}(t)$ suggests the level of trust nodes i is their neighbour j at time t. The degree of trust was restricted for continuous fractional value in range from 0 and 1 that refers the extended for that provided node believes that their adjacent node is trusted. When the trust level to a node is either 0 or nearby 0, it represents the whole distrust whereas the trust degree 1 or nearby 1, implies the trusted entity. An entire trust $T_{i,j}(t)$, is determined as weighted aggregated sum of 3 modules provided as:

$$T_{i,j}(t) = w_1 DT_{i,j}(t) + w_2 \frac{IT^s_{i,j}(t)}{N_j} \tag{2}$$

where $DT_{i,j}(t)$ signifies the degree of direct trust node i has for node j at time t using the node i's observation of packet forwarding behavior for node j. $IT^s_{i,j}(t)$ denotes the average degree of indirect trust node i attained by the recommendation from the neighbors(s) for node j at time t. N_J indicates a collection of neighbours for node j. The weight factor w_1 and w_2 gets allotted to $DT_{i,j}(t)$ and $IT^s_{i,j}(t)$ correspondingly, such that

$$w_1 + w_2 = 1, \;\; 0 \le w_1 \le 1 \; and \;\; 0 \le w_2 \le 1. \tag{3}$$

An indirect trust can be computed using the observation offered via the interaction with neighbors who notify regarding the direct observation for a specific node. The indirect trust $IT^s_{i,j}(t)$ can be computed by the following:

$$\sum\nolimits_{s \in N_j, s \neq i} IT^s_{i,j}(t) = \sum_{s \in N_j, s \neq i} DT_{i,s}(t) \times DT_{s,j}(t) \tag{4}$$

where $DT_{s,j}(t)$ denotes the degree of direct trust evaluated by node s for node j. $DT_{i,s}(t)$ denotes the direct trust among the nodes i and s. The usage of $DT_{i,s}(t)$ guarantees that the node offering recommendation is trusted chain mechanism.

The direct trust $DT_{i,j}(t)$ in Eq. (3), signifies the basic element of forming the trust model and assessed the behavior of the nearby nodes. To determine the direct trust, the packet forwarding ratio of a node can be computed as follows.

$$DT_{i,j}(t) = CF_{i,j}(t)[TR_{i,j}(t)]^{-1} \tag{5}$$

$CF_{i,j}(t)$ means total number of properly forwarder packets by node j at time t and $TR_{i,j}(t)$ denotes total number of received packets by node j from node i at time t. Based on the degree of trust value the nodes as ranked and the high level ranked nodes are selected when integrated to the route discovery process that aids in the selection of trusted notes in the active route and isolates the compromised/faulty nodes.

3.2.2 Routing in MAODV

Unlike traditional AODV routing, in this MAODV routing protocol the nodes initiate the process of RSA algorithm with the well-known OTPs to classify the malicious nodes present in the network when they receive the RREQ packet. The RSA algorithm stats with the calculation of two mathematical variables via the OTPs of authorised nodes which is expressed as:

$$\eta_i = otp_i^1 \times otp_i^2 \tag{6}$$

$$\sigma_i = (otp_i^1 - 1)(otp_i^2 - 1) \tag{7}$$

where η_i and σ_i are the two mathematical parameters introduced for node I, otp_i^1 and otp_i^2 are the pair of OTPs generated for node i. To perform encryption in the ith node a public key is chosen by the OTP-RSA condition which is given by:

$$\gcd(a_i, \sigma_i) = 1 \tag{8}$$

where a_i is the public key of ith node. From the chosen public key a_i the malicious nodes present in the network are identified using the following condition:

$$Node_i = \begin{cases} Normal, & if\ a_i = prime \\ Malicious, & if\ a_i \neq prime \end{cases} \tag{9}$$

Using Eq. (9) the malicious and normal nodes present in the network can be identified. If a node is identified as malicious the process will be repeated to select an alternate node. At the same time, when a normal node present in the network is detected, i.e., if the public key of ith node a_i is a prime number, then the private key of the ith node can be calculated by the following equation:

$$a_i P_i \equiv 1 \bmod(\sigma_i) \tag{10}$$

where P_i is the private key of ith node. Using Eqs. (8) and (10) the keys used to perform the encryption and decryption process in the ith node is given by:

$$K_E(i) = (\eta_i, a_i) \tag{11}$$

$$K_D(i) = (\eta_i, P_i) \tag{12}$$

Using the private and public keys the original data which is to be transmitted can be encrypted at the source node and decrypted at the destination node. The encryption process performed by the public key of the source node is given by:

$$E(I) = I^a \bmod \eta \tag{13}$$

where, I is the original data that has to be sent. If an intermediary node can conduct encryption using Eq. (13), it will send an RREP packet to the source node. The source node can determine an optimum path for data routing by receiving RREP packets. If more than one way is specified, the best path is picked by taking the trust value into account and the data packet is forwarded through the selected path. The forwarded data is sent through intermediary nodes to the final destination, where it is decrypted and the original data is received. The decryption procedure performed by the private key at the destination node may be represented as:

$$D(I) = I^P \bmod \eta \tag{14}$$

Eqs. (13) and (14) also satisfy the following condition given by:

$$D[E(I)] = I \text{ and } E[D(I)] = I,\ 0 \leq I \leq \eta \tag{15}$$

The MAODV routing protocol can be simply explained by the following steps.

MAODV Routing Protocol

Setup phase:

Initialize the number of nodes.

Identify the Source (S) and Destination (D) nodes.

Route discovery phase:

RREQ broadcasting from S

Initialize RSA

Check the condition for OTP-RSA using Eqs. (8) & (9)

Verification of OTP-RSA in nodes

Identification of Malicious nodes by failed OTP-RSA verification.

Select a path which satisfies OTP-RSA and nodes with highest trust values.

Reception of RREP from D

Data encryption by S

Data broadcasting from S to D through the selected path

Route maintenance phase:

Data forwarding by optimal route and Route maintenance

Data decryption by D

The MAODV routing protocol selects the optimal path for data forwarding by the utilization of OTP based RSA algorithm and Trust evaluation. The routing method is highly secure because of the data to be transmitted is encrypted before forwarded and only the authorized destination node can decrypt the data with its private key. Also the proposed routing starts only after verification of OTP-RSA condition which identifies the malicious nodes in the network and binds the data from the attacks.

4 Simulation Results

This section provides a brief experimental results analysis of the MAODV routing protocol with simulation setup and performance analysis.

4.1 Simulation Setup

The simulation of the MAODV routing protocol take place using MATLAB 2014a tool on a PC with Processor: Intel i3, Windows 8 OS, and 4GB RAM. In addition, the WSN platform t is created with the parameters given in the Tab. 1.

Table 1: Parameter setting

Parameters	Specifications
Number of nodes	50, 100, 200, 300, 500
Node placement	Random
Channel	Wireless
Simulation area	100*100 sq. m
Packet size	100 bytes
Simulation time	100 s
Packet generation rate	8 packet/s

4.2 Results Analysis

The experimental results of the MAODV routing protocol are presented here. The significance of the proposed routing protocol is presented by varying the sensor nodes present in the network (N = 50, 100, 200, 30, 500). Tab. 2 shows the results of the MAODV routing protocol in terms of Packet Delivery Ratio (PDR), Throughput, End to End (ETE) Delay, Energy Consumption, Jitter and Detection Accuracy.

Table 2: Simulation results of MAODV protocol

Parameters	Number of Nodes				
	N = 50	N = 100	N = 200	N = 300	N = 500
PDR (%)	98.7	98.5	98.1	97.2	97.7
Throughput (bits/s)	6265	25580	100815	121587	178480
Detection Accuracy (%)	80	88.46	97	98	99
Energy Consumption (J)	49.99	49.96	49.93	49.87	47.03
ETE delay (s)	0.0074	0.0075	0.008	0.0082	0.0085
Jitter (s)	0.24	0.25	0.3	0.32	0.35

The performance of the MAODV routing protocol is evaluated by varying the sensor nodes as N = 50, 100, 200, 300 and 500 which is shown in Fig. 2.

Figure 2: Performance of MAODV protocol

Fig. 2 shows that the PDR of the MAODV routing protocol is significantly greater even the node count present in the network is high. It is evident that the PDR value for the proposed routing protocol ranges about 97% to 98 % since the node count varies from 50–500 which proves that the routing protocol trust worthy.

4.3 Performance Analysis

PDR: It is defined as the ratio of number of data packets effectively reached at the receiver to the number of packets sent by the transmitter node. It can be defined as follows:

$$\%PDR = \frac{nP_{receieved}}{nP_{transmitted}} * 100 \tag{16}$$

where $nP_{transmitted}$ is the number of packets sent, $nP_{receieved}$ is the number of packets received.

Throughput: It represents the amount of the successful transmission of data from source to destination, as defined below.

$$Throughput = \frac{nP_{transmitted}}{nP_{transmitted} + nP_{lost}} \tag{17}$$

where $nP_{transmitted}$ is the total number of packets sent, nP_{lost} is the total number of packets lost at the time of transmitting data.

ETE delay: The average sum of the difference delay of data packets reached at the destination and data packet transited by the source. It can be equated using Eq. (18):

$$E2E\ Delay = \frac{nP_{received}(T_{received} - T_{transmission})}{nP_{received}} \tag{18}$$

where $nP_{receieved}$ is the number of packets received, $T_{received}$ is the time when data packet received by the destination, is the time when data packet sent by the source.

Detection Accuracy: It is defined as the ratio of the number of detected malicious nodes and the total number of malicious nodes exist in the network. It can be defined as follows:

$$\%D(Accuracy) = \frac{nM_{Detected}}{M_{Total}} * 100 \tag{19}$$

where M_{Total} denotes the malicious node count in the network and $nM_{Detected}$ indicates the number of identified malicious nodes.

Energy Consumption: It represents the quantity of energy spent by the network to transmit the data and is calculated as follows:

$$E_{consumption} = \begin{cases} E - (E_T + E_{DA})(packetsize) + E_{amp}Packet \times d^4, & d > d_0 \\ E - (E_T + E_{DA})(packetsize) + E_{fs}Packet \times d^2, & d < d_0 \end{cases} \tag{20}$$

where E is the initial energy, E_T is the energy of transmitted data, E_{DA} is the energy of aggregated data, E_{fs} is the free space energy, E_{amp} is the energy dissipated by the power amplifier, d is the distance between the source and destination, and d_0 can be computed as:

$$d_0 = \sqrt{\frac{E_{fs}}{E_{amp}}} \tag{21}$$

4.4 Performance Comparison & Discussion

With the intention to show the superiority of the MAODV routing protocol than the existing routing protocols namely AODV, LAR1, OLSR and ZRP. A detailed comparison study is made in terms of Throughput, PDR, Energy consumption, ETE delay and Detection Rate. Fig. 3 shows offers the comparison study of the MAODV protocol in terms of Throughput with $N = 100$.

Fig. 3 shows that the MAODV routing protocol achieves the throughput close to 6000 bits/s which is significantly greater than the throughput of AODV routing protocol which is close to 4000 bits/s.

The delay usually occurs owing to the process of route discovery, queuing, propagation and transfer time. The average ETE delay achieved by the MAODV routing protocol is shown in Fig. 4.

From Fig. 4 it is clearly observed that the Average ETE delay achieved by the MAODV routing protocol is 0.05 s which is lower when compared AODV routing protocol with ETE delay of 0.2 s. The proposed AODV protocol uses the modified packet structure with passing the nodes with lower buffer rate, which decreases the delay period and extends the network lifetime.

The malicious node detection against selective forward attack in the network is the primary goal of the study. With such intention, the accuracy of malicious node detection is one of the main parameters to be considered for performance evaluation.

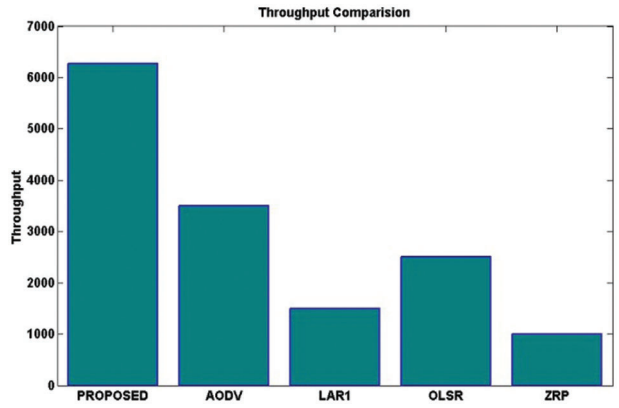

Figure 3: Throughput analysis of proposed and existing techniques

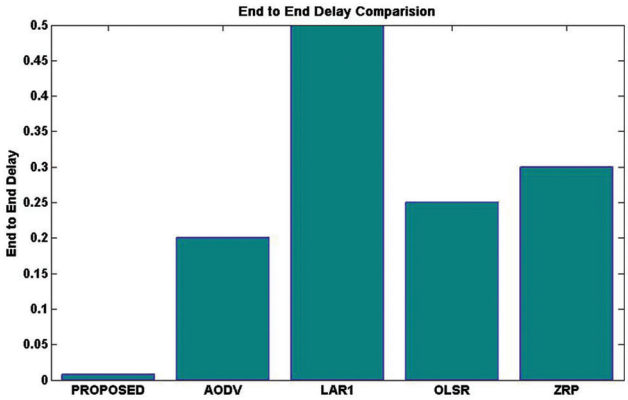

Figure 4: ETE delay analysis of proposed and existing techniques

Fig. 5 showcases the comparison study of the routing techniques based on detection Accuracy. The MAODV routing protocol achieves 88.46% detection accuracy with $N = 100$ which is comparatively higher than the detection rates of existing protocols like AODV, LAR1, OLSR and ZRP. Existing protocols requires more energy for the prediction of malicious nodes.

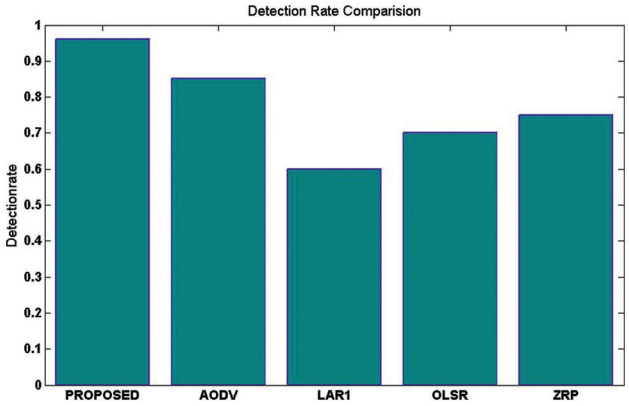

Figure 5: Comparative results analysis in terms of detection rate

The PDR achieved by the MAODV routing protocol is depicted in Fig. 6. The presented MAODV routing protocol achieves PDR close to 98% with $N = 100$ which is higher than the existing protocols. Since AODV routing protocol achieves 50% PDR, LAR1 achieves 40% PDR, OLSR achieves 38%, and ZRP achieves 30% PDR. This means that the trust evaluation for malicious nodes prediction is helpful in improving the packet delivery ratio and the direct and indirect trust evaluation helps in the trust computation.

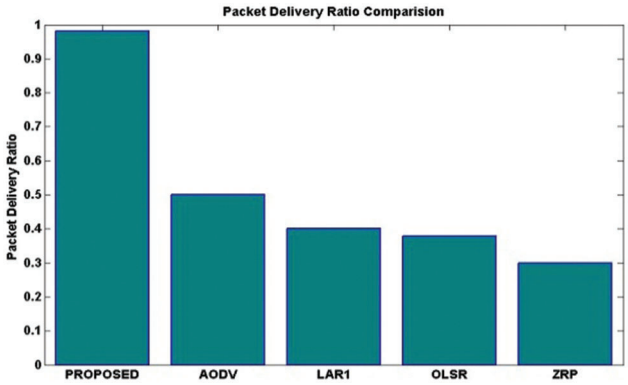

Figure 6: Performance comparison in terms of PDR

Generally, energy is an important parameter used to maintain the functioning of the nodes during transmission and reception. The energy consumption achieved by the MAODV routing protocol is depicted in Fig. 7.

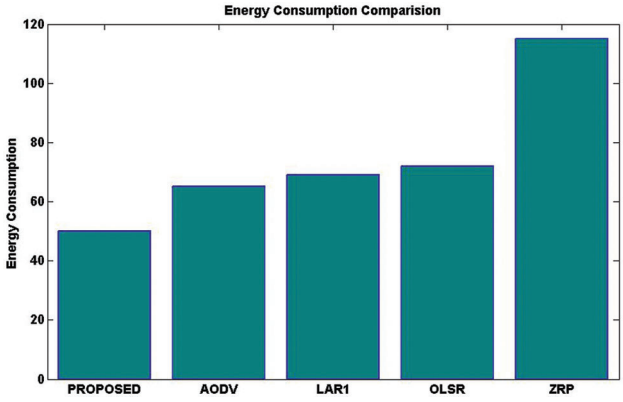

Figure 7: Energy consumption of MAODV routing protocol

Demonstrates the reduction in energy consumption of the routing protocol compared to other existing protocols. It is observed that the proposed routing protocol obtains a maximum of 49.49 Joules energy consumed by the network with $N = 100$ which shows that the energy utilization of the proposed routing protocol is lower compared to the existing protocols.

5 Conclusion

In this article, we have given a concept for a novel routing protocol based on RSA and OTP verification to ensure that data transfer is safe and dependable. The presented modified version of the basic AODV routing protocol allows for detecting malicious nodes by utilizing the RSA algorithm at the beginning of the routing process. This simplifies and improves the reliability of the routing process while also making it more secure and reliable. In addition, the suggested routing protocol minimizes the computational cost. It

optimizes the selection of the route to be used for data transmission depending upon the trust value. Furthermore, the outcomes of the simulations are provided in terms of several performance assessment parameters in this paper. The comparisons presented in this article demonstrate that the suggested routing protocol may be the protocol of choice in the future when it comes to protecting networks against selective forward assaults.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Z. Khan, Y. Xiang, M. Y. Aalsalem and Q. Arshad, "The selective forwarding attack in sensor networks: Detections and countermeasures," *International Journal of Wireless and Microwave Technologies (IJWMT)*, vol. 2, no. 2, pp. 33–44, 2012.

[2] J. Jiang, G. Han, F. Wang, L. Shu and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[3] A. Prathapani, L. Santhanam and D. P. Agrawal, "Detection of blackhole attack in a wireless mesh network using intelligent honeypot agents," *The Journal of Supercomputing*, vol. 64, no. 3, pp. 777–804, 2013.

[4] J. Wang, Z. Liu, S. Zhang and X. Zhang, "Defending collaborative false data injection attacks in wireless sensor networks," *Information Sciences*, vol. 254, no. 7, pp. 39–53, 2014.

[5] I. Khalil, S. Bagchi, C. N. Rotaru and N. B. Shroff, "UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks," *Ad Hoc Networks*, vol. 8, no. 2, pp. 148–164, 2010.

[6] M. Conti, R. Di Pietro, L. Mancini and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 685–698, 2011.

[7] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Computers & Electrical Engineering*, vol. 40, no. 2, pp. 530–538, 2014.

[8] B. Zhu, S. Setia, S. Jajodia, S. Roy and L. Wang, "Localized multicast: efficient and distributed replica detection in large-scale sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 913–926, 2010.

[9] Z. A. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks," *Computer Communications*, vol. 34, no. 3, pp. 468–484, 2011.

[10] S. K. Stafrace and N. Antonopoulos, "Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks," *Computer Communications*, vol. 33, no. 5, pp. 619–638, 2011.

[11] Y. Ren, M. C. Chuah, J. Yang and Y. Chen, "Detecting wormhole attacks in delay-tolerant networks [Security and Privacy in Emerging Wireless Networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 36–42, 2010.

[12] S. Hamedheidari and R. Rafeh, "A novel agent-based approach to detect sinkhole attacks in wireless sensor networks," *Computers & Security*, vol. 37, pp. 1–14, 2013.

[13] S. Sultana, G. Ghinita, E. Bertino and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet dropattacks in wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 3, pp. 256–269, 2015.

[14] S. Khanam, H. Y. Saleem and A. S. K. Pathan, "An efficient detection model of selective forwarding attacks in wireless mesh networks," in *Int. Conf. on Internet and Distributed Computing Systems, IDCS 2012. Lecture Notes in Computer Science*, vol. 7646, Malaysia, Springer, Berlin, pp. 1–14, 2012.

[15] I. D. Chakeres and E. M. Belding-Royer, "AODV routing protocol implementation design," in *Proc. of the 24th Int. Conf. on Distributed Computing Systems Workshops, 2004. Proceedings, 2004*, Tokyo Japan, pp. 698–703, 2004.

[16] T. Sreelakshmi and G. S. Binu, "Energy efficient detection-removal algorithm for selective forwarding attack in wireless sensor networks," in *Int. Conf. on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, Kottayam, India, pp. 1–6, 2018.

[17] M. H. Shinde and D. C. Mehetre, "Black hole and selective forwarding attack detection and prevention in WSN," in *Int. Conf. on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, pp. 1–6, 2017.