SECURED AODV TO PROTECT WSN AGAINST MALICIOUS INTRUSION

Saad Al-Ahmadi and Abdulrahman Alseqyani

Department of Computer Science, King Saud University, Riyadh, Saudi Arabia

ABSTRACT

One of the security issues in Wireless Sensor Networks (WSN) is intrusion detection. In this paper, we propose a new defence mechanism based on the Ad hoc On-Demand Vector (AODV) routing protocol. AODV is a reactive protocol designed for ad hoc networks and has excellent flexibility to be adapted to a new secure version. The main objective of the proposed secured AODV routing protocol is to protect WSN against malicious intrusion and defend against adversary attacks. This secured AODV protocol works well with the WSN dynamics and topology changes due to limited available resources. It establishes secure multi-hop routing between sensor nodes with high confidence, integrity, and availability. The secured AODV utilizes an existing intrusion dataset that facilitates new collection from all the exchanged packets in the network. The protocol monitors end to end delay and avoid any additional overhead over message transfer between sensor nodes. The experimental results showed that this secured AODV could be used to fight against malicious attacks such as black hole attacks and avoid caused large transmission delays.

KEYWORDS

Intrusion Detection, Wireless Sensor Network, Security, Attack, AODV

1. INTRODUCTION

Wireless Sensor Network (WSN) defined as "a small scale gathering nodes of a sensor used for monitoring, sense, capturing and processing the data around an application" [1]. WSN usually consists of different sensor nodes that communicate with each other and with the base station, as it appears in Figure 1. The sensor node consists of different components, which are Power Supply, Sensor, Processing Unit, and Communication System.

Because of enormous applications for WSN, the security issues are a big concern for users and researchers. These different applications contain Battlefield Management and Surveillance, Biomedical Applications, Disaster Management, Environment Control and Monitoring, Personal Health Care, and Weather Sensing. The two types of security attacks can make big threats to WSN, which are: active attacks and passive attacks [2]. Passive attacks concern with unauthorized attackers who can communicate and listen to the channel between the sender and receiver. Some of these frequent attacks target privacy issues such as monitoring, eavesdropping, traffic analysis, and camouflage adversaries. Active attacks are more dangerous than passive because they may affect the transmitted data by changing its information or modify it. Routing attacks, physical attacks, message corruption, and Denial of Service (DoS) is the most known active attacks in WSN.

WSNs tend to be vulnerable to different kinds of security threats and attacks, which can prevent the network performance and result in the sensors sending wrong information or message to the sink [3]. Primary management, secure, and authentication protocols cannot guarantee the level of

DOI: 10.5121/ijnsa.2020.12501

security necessary for WSNs. Intrusion Detection System (IDS) is required to provide a lasting solution to the problem through network analysis for the detection of abnormal sensor node(s) behavior. In WSNs, a routing protocol for better detection of attacks and classifications is necessary, and one of them is the Ad Hoc On-Demand Vector (AODV) routing protocol. In [4], AODV is a routing protocol designed for wireless ad hoc networks, and it operated when a source node requires a 'route' to an intended destination [5].

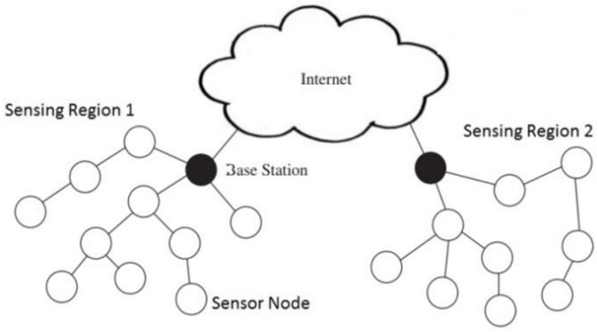

Figure 1. Wireless Sensor Network architecture

The intrusion process initiated by an attack conducted using foreign or inside exploitation. Intrusion detection divided into two classes: signature-based detection and anomaly-based detection. Signature-based detection uses unique signatures whereby invaders identify the system's weakness and thus find a way of getting into the system. The second class of intrusion detection is anomaly-based detection. It is based on the fact that normal behavior can be defined so that intrusion behavior is considered an anomaly and can be detected [6]. Regular attacks are two turn attacks; the two turn attacks are not sturdy and do not significantly impact the network structure. In the network structure, regular attacks are the primary cause of damage in the structure. There is an indication of the weaknesses in the network structure. Furthermore, they show the network weaknesses and the areas the network structure is likely to face attacks.

2. LITERATURE REVIEW

A research work studied the challenges of intrusion and presented Decentralized rule-based IDS as a reliable technique that fits the networks' demands and restrictions. This type of method can detect several attack routes, including black-hole, delay attacks, selective-forwarding, and worm-hole. Ideally, rule-based intrusion detection is a kind of system that can typically learn the activities of a given machine or specific network and ultimately detect new or any kind of attack. It mainly incorporates three phases: acquisition of data, application of the rule, and detection of intrusion. It is important to note that the simulation result undertaken by the researchers has revealed how the method is very efficient and ultimately accurate in the detection of various kinds of simulated attacks [7].

On the other hand, it can also present visualization technology, which has helped make detection more effective compared to traditional techniques. The research is more in-depth and has more visual experiments as compared to rule-based research. However, despite the credibility and the reliability of automatic detection systems, anomalous activity detection is unreliable in automated systems. In this regard, the authors designed a unique mechanism for visual network presentation. The technique has allowed the operators to analyze data visually. The results obtained from using this type of technology are significant. The visualization of data reduces the amount of time and effort required in identifying complicated kinds of patterns and their prospective relationships [8].

Similarly, it has shown improvements that can be made in the sensor node to make it more efficient and reliable. It is essential to note that there have been substantial faults in sensing systems over the years. As such, the reliability and effectiveness have emerged as one of the critical issues in the WSN research studies, mainly because, most often than not, the sensor nodes deployed in an unattended and unfavorable environment. The research has presented sensing improvements that can improve the reliability, sensibility, and effectiveness of the system. The research shows and analyzes the impact of sensing improvements of IDS [9].

Another mechanism is proposed by [10], who came up with a rather quick detection of intrusion in WSN by minimizing the number of active nodes. The designers faster this mechanism of intrusion detection by designing the mechanism problem as a Markov Decision Process (MDP). In this case, the established work is a fusion center based on MDP and one that chooses the appropriate number of sensors needed to be switched on after each period of time. The proposed algorithm tries to avoid false alarms, which cause energy consumption and time delay. It can detect problems in the system using observations of the minimal amount and minimize the number of nodes active.

Protecting ad-hoc networks from intrusion attacks requires a multi-prolonged strategy. They are preventing intrusion in the form of reliable identification, and authentication mechanisms alone are not enough. Malicious intrusion can still occur in the form of attacks both inside and outside the network environment, which can comprise and weaken the integrity of the network leading to severe consequences. Intrusion detection is often done by the comparison of the system when intrusions are absent. Therefore, a fundamental assumption is that both normal and abnormal behaviors of the system can be characterized. The community of intrusion detection concentrates mainly on wired networks [11]. However, the techniques directed at wireline networks would not emerge or occur since the environment made up of multi-hop wireless connections. The main differences between the wired and wireless networks are lack of mobility, fixed infrastructure, ease of listening to wireless transmissions, and lack of clear distinction between normal and abnormal behaviors. Additionally, the conventional network approaches to detecting network approaches to network intrusion detection primarily based on the frequent presence of specific yet common pinch points at a few dedicated intrusion platforms for monitoring all traffic [2].
Routing in ad hoc networks faces numerous challenges like mobile nodes, decentralized systems, low infrastructure, limited and medium challenge, more power required, and malicious nodes. These challenges cause significant routing performance degradation. Based on the information available and broadcasted by other nodes, there is an update of routing tables. AODV presents a source of the on-demand routing protocol initiates [11]. The collected AODV routing data is done based on the request, and the route is decided based on network queries.

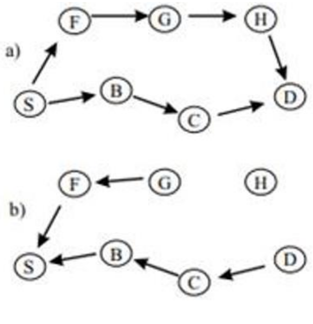

Figure 2. Route Discovery in AODV

ADOV adopts sequence numbers to establish and determine the routing information freshness and ensure the presence of loop-free routes [3]. The presence of multiple routes results in a node selecting a route with the highest sequence number. Instances where there are similar sequence numbers, the node chooses the route with shorter hop-count. The route entries kept fresh using timers. In [3], it found out that AODV periodically sends 'Hello' messages to ensure the information remains updated concerning the neighboring nodes' connectivity.

The specific security mechanisms, like strong authentication, are not incorporated by the AODV protocol. Therefore, there are instances where mischievous behaviors occur as there is an obvious way for their prevention. Some of these behaviors include IP spoofing, MAC spoofing, and dropping packets, including the alteration of contents making up the control packets. Some proposed protocols in the literature, such as SAODV and SAR designed to protect AODV against some malicious attacks at the expense of performance, latency, and overhead [4].

IDS mechanism introduced in [12] for identifying routing attacks in Wireless Sensor Networks. In this solution, all nodes must have the installed IDS agent to allow the detection of anomalies. The various identified fields in the IDS for the mechanism include different things such as the total number of received or sent packages and the route request sent or received or established. Each node employs these different categories for shaping the standard deviation of standard messaging by each neighboring node. A fixed width cluster formed depending on the result of the standard deviation of each node. Compromised nodes can be determined based on cluster analysis.

Cryptography is another mechanism for avoiding or at least minimizing the external attacks that target the Wireless Sensor Network. It can guarantee that different security services such as authentication and integrity by examining the source and contents of data packet using numerous methods such as symmetric encryption, public-key cryptography, and hash functions [13][14]. This research illustrates how cryptography employed in securing the WSN from external kinds of attacks. The numbers of experiments performed are average as compared to the other research. As the main objective of the experiments and the study, in general, was to be able to come up with an intelligent intrusion detection technique that can prevent DoS kind of attacks within a reasonable cost limit regarding energy and processing. The results of the experiments found out that the DoS attacks are relatively high. As such, emphasis on identifying and considering security attacks early enough in the network protocol development process is important.

Another recently proposed works on Intrusion Detection System in Wireless Sensor Network was surveyed by [15], who established different Intrusion Detection System approaches based on their detection techniques. The approaches based on the following: misuse detection, specification-based detection protocols, and anomaly detection. It indicated Intrusion Detection System protocols needed to tackle the current Wireless sensor network's security attacks. An analysis carried on network structure about Wireless sensor network, and the results showed that Intrusion Detection System had critical shortcomings which defined the future of research this platform. One of the proposed works included smart grids.

Smart grids are new when it comes to intelligence, efficiency, and optimality to power grids. Many changes occurring on the Internet, like communications networks, use a top a current power grid that comprises wireless mesh network technologies with 802.15.4, 802.11, and WiMAX standards. It leads to the power grid's exposure by each of these wireless mesh network technologies to cybersecurity threats.

These issues were addressed by [16] who proposed Distributed Smart Grids of IDS (SGDIDS) by creating as well as deploying an intelligent module known as Analyzing Module (AM), in a wide range of smart grid layers. Numerous Analyzing Modules fixed at all levels of a smart grid, which include Wide Area Networks (WANs), Home Area Networks (HANs), and Neighborhood

Area Networks (NANs). It allowed Artificial Immune System (AIS) and Support Vector Machine (SVM) to detect and classify the type of cyber-attacks and the type of malicious data injected in Wireless Sensor Networks and this achieved by training Analyzing Modules at all levels.

3. METHODOLOGY

3.1. Proposed Method

AODV is an improvement of the Dynamic Destination-Sequenced Distance-Vector (DSDV) routing protocol. However, AODV is a reactive routing protocol instead of being proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes, in turn, broadcast the packet to their neighbors, and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the neighbor's address from which the first copy of the broadcast packet received. This record stored in their route tables, which helps in establishing a reverse path. If additional copies of the same RREQ are later received, these packets discarded. The reply sent using the reverse path. For route maintenance, when a source node moves, it can reinitiate a route discovery process. If any intermediate node moves within a particular route, the drifted node's neighbor can detect the link failure and send a link failure notification to its upstream neighbor. This process continues until the failure notification reaches the source node. Based on the received information, the source might decide to reinitiate the route discovery phase.

The AODV algorithm allows self-starting and multi-hop routing between mobile nodes willing to create and maintain a network. AODV permits mobile nodes to get routes rapidly for new destinations and, at the same time, does not require nodes to maintain routes to inactive destinations. In the case of link breakage or network topology change, AODV mobile nodes will respond on time. The operation of AODV is loop-free, and when a node moves in the network, it offers quick convergence. When links break, AODV causes the affected set of nodes to be notified so that they can overturn the routes using the lost link. One distinguishing feature of AODV is its use of a destination sequence number for each routing table entry. The destination sequence number created by the destination and included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given a choice between two routes to a destination, a requesting node is required to select the one with the highest sequence number [17].

There are different methods used in the neural network; optimization algorithms used in the learning process. Several algorithms used in the optimization process include; Newton method, gradient descent, Conjugate gradient, and Levenberg algorithms. Some of the methods used in recognizing the relationship between the datasets. The process involves mimicking the human brain, mimicking the exact way the human brain operates. Under the methods, some neurons are either artificial in nature or organic. The primary purpose of the neural networks is to understand the data patterns. The patterns also recognized in future data samples; the purpose is making future predictions on similar data [18].

3.2. Experiment

As shown in Figure 3, when forwarding the RREQ message, each intermediate node updates its routing table and adds a "reverse route" entry to s, indicating via which next-hop the nodes reached, and the distance in the number of hops. Once the destination node d receives the first

RREQ message (we assume via a), d also adds a reverse route entry in its routing table, saying that node s reached via node a, at a distance of 2 hops. Node d then responds by generating a route reply (RREP) message and sending it back to node s. In contrast to the RREQ message, the RREP is unicast, i.e., it is sent to an individual next-hop node only. The RREP is sent from d to a, and then to s, using the reverse routing table entries created during the forwarding of the RREQ message. When processing the RREP message, a node creates a "forward route" entry into its routing table. For example, upon receiving the RREP via a node, s creates an entry saying that node d reached via a, at a distance of two hops. After the route discovery process, a route established from s to d and data packets can start to flow. In the event of link and route breaks, AODV uses route error (RERR) messages to inform affected nodes. Sequence numbers, another vital aspect of AODV, indicate the freshness of routing information. AODV uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages). Nodes maintain their sequence number as well as a destination sequence number for each route discovered. This use of sequence numbers can be an efficient approach to address the problem of routing loops but has to be taken with caution since loop freedom cannot be guaranteed a priori.

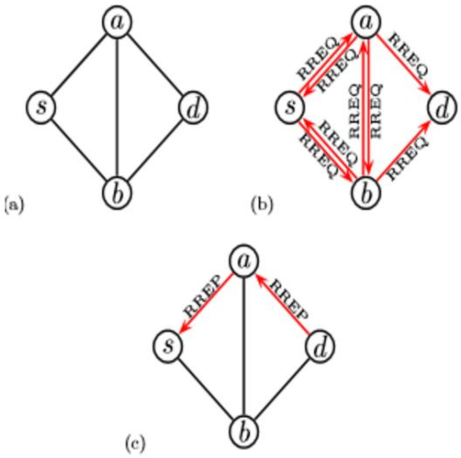

Figure 3. Network Topology Example

The main aim of improving AODV is to make sure that the data packet loss is reduced or wholly managed. Several techniques can be employed or used to prevent the data packet loss in AODV protocol. The techniques discussed below.

a) Nth Backup Route (AODV nthBR) Technique

The Nth Backup Route techniques provide backup routes in the AODV environment. This technique helps the protocol to find the nearest node to the failed node [19]. Therefore, there will be zero packets lost due to nodes failure, and the packet does not problem finding a node. This technique also helps to check whether the node has enough energy to transmit the packet. The node that has enough energy is selected to transmit that packet, and the route completed.

b) Pre-request Receive Reply Technique

The following is an algorithm of pre-request receive reply technique at the source node.

```
Receive Reply (Packet P)

    if (P has an entry in Route Table)
```

```
            select Dest_Seq_No from routing table
            if (P.Dest_Seq_No > Dest_Seq_No)
                  update entry of P in routing table,
                  unicast data packets to the route specified in RREP
            else
                  discard RREP
      else
            if (P.Dest_Seq_No ≥ Src_Seq_No)
                  Make entry of P in routing table
            else discard this RREP
```

Therefore, the source code will ensure that packet is not lost because it will be able to destroy all the malicious requests that are done in the source nodes.

c) Using Digital Signatures and Hash Functions

These are mainly used to enhance the security and performance of AODV protocol under the black hole attack. Packets will be sent with digital signatures whereby the receiving nodes will be able to tell that a particular packet is from a specific source node. This digital signature is associated with a unique ID on the packet head of the message [20].

With hash functions, it involves encrypting the message using a source code that can only be decrypted by the node with the key.

An example of message pseudo-codes sending RREQ is whenever a source wants to send the data, it broadcasts or floods the RREQ

```
      if (route does not exist)
            Check cache for already existence request that is sent for destination
            if (the request has not been sent already)
                  Create a RREQ packet
                  Add (dest addr, broadcast ID) to cache
                  broadcast RREQ locally
                  the timer is set for RREP_WAIT_TIME for rebroadcasting RREQ
                  Increment broadcast ID
```

d) Secure AODV

Secure AODV can be used to improve AODV in a mobile network. It is an extension of the AODV routing protocol used to protect route discovery by providing key security features like non-repudiation, authentication, and integrity [21]. This Improved Protocol (SAODV) assumes that each node has a signature key pair from a suitable asymmetric cryptosystem. Also, the nodes in SAODV are capable of verifying the association between the address of a given node in that network and the public key associated with the node.

e) Using Data Structure Algorithms for Path Compression

This technique operates in a promiscuous mode whereby the nodes in this network disable the MAC address and therefore, can listen to all the packets within their radio range. This technique also considers the source and destination hop-count before compressing the paths [22]. When a node in the network has a packet for a destination, it gathers all the necessary information and identifies a route; then, the node listens promiscuously to a data packet. It takes action depending on whether it is an active route or not.

4. Results And Analysis

Assuming that m nodes transmitting a message during routing discovery, as the AODV protocol says, if the first routing discovery was right, the routing node number of transmitting control message is:

$$AODV(m) = m - 1 + t$$

where, t is the number of nodes transmitting routing reply message. If there was more than one time during routing discovery in AODV, then it should be:

$$AODV(m) = c\ (m-1+t)$$

where c meant the number of routing discovery process. If data transmitted following Bus AODV (B-AODV), there was at least one stable routing to be found to transmit data during routing discovery, so only 2m-2 nodes were deeded to transmit data:

$$B\text{-}AODV(m) = o(2m-2)$$

from this we can conclude: when $c > 1$, AODV protocol produces much more routing overhead in the routing building process.

Performance Metrics & definitions:

- Packet Delivery Ratio (PDR): is a ratio of the number of packets received by destination to the number of packets sent by the source.
- End to End Delay: in seconds; is the time it takes a data packet to reach the destination.
- Throughput: is the rate of successfully transmitted data per second in the network during the simulation.
- Routing overhead (RH): is the total number of routing packets/ Total number of delivered data packets.
- CH: Cluster Head
- ADV-CH: is the advertisement message broadcasted by each CH to the rest of the nodes using CSMA-MAC.

4.1. Dataset Description

In building a dataset and collecting the necessary data from all the sent and received packets in the WSN, it is essential to note that monitoring assistance and service needed, whereas ensuring a minimum cost. Similarly, it is essential to ensure that the necessary and relevant data that will help in detection, classification, and the prevention of the different possible attacks are seemingly collected. In this specific research, to distribute the load among the various sensor nodes, each sensor will be part of the monitoring process and should consequently be in a capacity to monitor the set of its neighbor. The biggest challenge experienced in this phase was determining the appropriate number of nodes that can be watched by a given sensor node to monitor all the network sensors herein. Many such experiments have been initiated in quest of determining the number of nodes, and the results of the experiment explained below.

The used dataset collected from the modification of the AODV protocol. For instance, malicious nodes are expected to be detected at the initial stage and immediately removed to prevent it from taking part in the advanced process. The dataset set must be analyzed in a unique, sequential manner to facilitate the immediate identification of malicious nodes. The unique sequential numbers are also simulated and are also based on the use of varying features that detect intrusion. For instance, by analyzing the dataset, it makes it easy to explore such features, namely system file comparison of data against malware signature, processes of scanning to detect signs of harmful patterns, monitor user behaviors for detecting malicious intent, and settings and configurations for the monitoring system. These features are essential. Thus, the dataset below is studied based on patterns in line with the Packet Delivery Ratio (PDR).

4.2. Packet Delivery Ratio versus Throughput

The Packet Delivery Ratio (PDR) is the ratio of packets successfully received to the total sent. Throughput is the rate at which information sent through the network [23]. If a network becomes congested and there is good discipline, packets may queue up at the source and never enter the network. Those packets will not contribute to throughput, but they will not affect the PDR at all because they are never sent.

Therefore, the PDR calculated as follows:

PDR=Total number of packets received / Total number of packets sent

On the other hand, Throughput is measured in kilobytes/s and is calculated as follows:

Throughput (Kbps) =Total packet size received * 8 / Total simulation time

Table 1 shows the relationship between PDR and throughput. It can be seen from Table 1, throughput increases across all the nodes. Therefore, increasing the number of nodes increases throughput and vice versa. Thus, the average rate of successful packet delivery will improve with an increase in throughput.

Table 1. Packet Delivery ratio and Throughput.

No. of Nodes	**Packet Delivery ratio**	**Throughput**
1	1	0.006668
2	0.980403	0.006736
3	1	0.006768
4	1	0.006777
5	1	0.006868
6	0.999732	0.006875
7	0.980403	0.006936
8	1	0.007668
9	1	0.007668
10	0.027915	0.007736

4.3. End to End Delay and Routing Overhead

End to End Delay EED(s) is the time taken to transfer a packet from one sensor node to the next one [24] and it is calculated as follows:

EED(s) = (Arrival Time - Sent Time) / Total Number of Connections
How EED occurs:

- The actual time taken to transfer the packet through the network.
- Since the packets being transmitted are so many, a delay can occur due to queuing of the packets as they wait for free slots to be created. This can happen when a packet is lost or transferred to the next node.
- Propagation Delay-This is the actual time taken by the bits to move from one node to the other.
- Processing Delay- The router takes time also to process the time, distance, and nodes where the packets will be transferred to also.

Table 2 shows EED from the simulation and throughput. From the table above, we can see, as the number of nodes increases, the average EED increases for all cases. Therefore, in dense network, there is high EED, therefore an increase in packet loss which in turn leads to low performance of the network. The EED is demonstrated in Figure 3 which shows a curve that rises where the number of nodes increases.

Table 2. End to End Delay and Throughput.

No. of Nodes	End to End Delay	Throughput
1	0.027915	0.000536
2	0.044079	0.003281
3	0.051683	0.001071
4	0.068415	0.002669
5	0.081688	0.001605
6	0.098964	0.007216
7	0.13806	0.00647
8	0.14703	0.002403
9	0.16701	0.002669
10	0.27915	0.000536

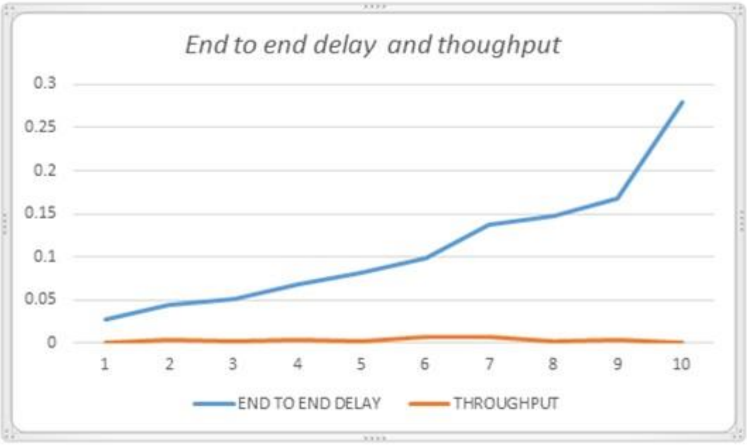

Figure 3. End to End Delay and Throughput

4.4. Routing Overhead

Routing overhead refers to metadata and network routing information sent by an application, which uses a portion of the available bandwidth of a communications protocol [25][23]. This extra data, making up the protocol headers and application-specific information, is referred to as overhead since it does not contribute to the content of the message.

In a similar manner in a network, when nodes exchange routing information using the same bandwidth used by data packets, incur overhead to the network referred to as Routing Overhead as this information packets are exchanged periodically in certain intervals of time. One example can be the Hello packets or the Keep-Alive packets, which are not the data packets but consume the bandwidth of the network, causing overhead to the network.

Routing Overhead calculated as follows:

Routing Overhead RH (bytes) = number of routing packets generated / Total number of packets generated.

Figure 4 below shows a screenshot results obtained from the dataset for Routing Overhead. The graph forms a slanting curve. This is the result of the increase in sensor nodes, which increases the number of routing packets generated and hence more nodes means more packets communicated between the packets. Therefore, an increase in nodes causes an increase in routing packets sent and received.

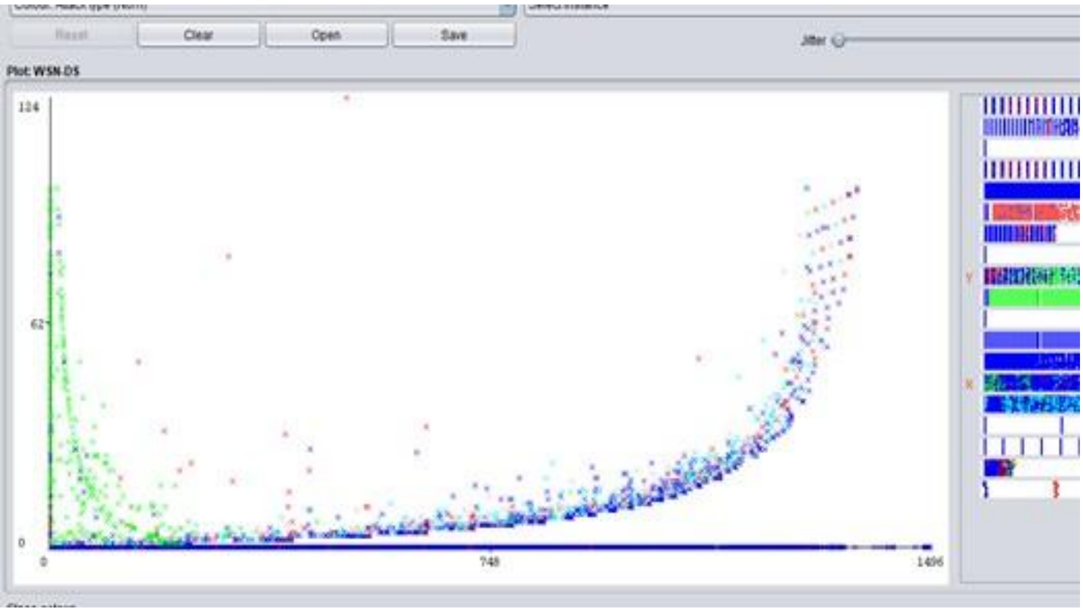

Figure 4. Routing Overhead

4.5. Time and Data (Packet) Received

Figure 5 below shows a result obtained after running a simulation using Weka software, and it describes the relationship between time and packets received. From Figure 5, we can see that as time increases, the number of packets received also increases significantly. There is also a decrease of packers received as the time increases more and more, this is due to packet loss as they wait for free slots or during the transfer from one node to the other.

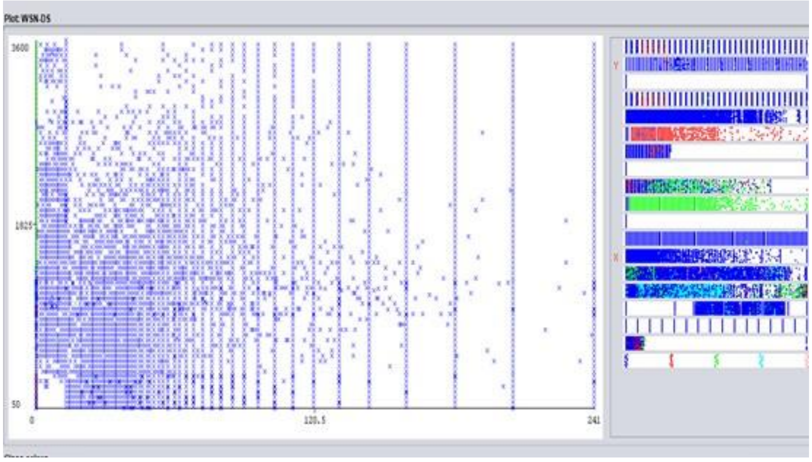

Figure 5. Time versus Data received in Weka

5. Conclusions

In the DSDV routing protocol, mobile nodes periodically broadcast their routing information to the neighbors. Each node requires to maintain their routing table. AODV protocol finds routes by using the route request packet, and the route discovered when needed. The comparison of these protocols made with the parameters packet delivery ratio, throughput, end to end delay, routing overhead. AODV performs better than DSDV in packet delivery ratio, throughput, and routing overhead. The delay of AODV is more than DSDV. The performance of AODV gets affected by the black hole attack. It reduces the packet delivery ratio and throughput to zero, and hence modifications are done in AODV, which gives better results even in the presence of the black hole attack. Packet delivery ratio and throughput in case of AODV and AODV after modifications are the same. However, for modifications, new packets are added in routing, and hence routing overhead is more than AODV without modification.

References

[1] C. Worlu, A. A. Jamal, and N. A. Mahiddin, “Wireless Sensor Networks, Internet of Things, and Their Challenges,” Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 12S2, pp. 556–566, 2019.

[2] N. A. Alrajeh, S. Khan, and B. Shams, “Intrusion detection systems in wireless sensor networks: A review,” Int. J. Distrib. Sens. Networks, vol. 2013, 2013.

[3] R. Khan ShahSani, M. Bakhsh, and A. Mahmood, “Performance Enhanced AODV Routing Protocol Security in Mobile Ad-Hoc Networks,” Int. J. Technol. Diffus., vol. 3, no. 3, pp. 57–70, 2013.

[4] P. Ning and K. Sun, “How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols,” Ad Hoc Networks, vol. 3, no. 6, pp. 795–819, 2005.

[5] W. A. Aliady and S. A. Al-Ahmadi, “Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks,” IEEE Access, vol. 7, pp. 84132–84141, 2019.

[6] P. Wanda, “A Survey of Intrusion Detection System,” Int. J. Informatics Comput., vol. 1, no. 1, pp. 1–10, 2020.

[7] A. Paula, R. Silva, M. H. T. Martins, A. A. F. Loureiro, and L. B. Ruiz, “Decentralized intrusion detection in wireless sensor networks Decentralized Intrusion Detection in Wireless Sensor Networks,” no. June 2014, 2005.

[8] E. D. Thomas et al., “Intrusion detection and monitoring for wireless networks.,” 2005.

[9] M. T. Hsu, F. Y. S. Lin, Y. S. Chang, and T. Y. Juang, “The reliability of detection in wireless sensor networks: Modeling and analyzing,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 4808 LNCS, pp. 432–443, 2007.

[10] K. Premkumar and A. Kumar, “Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks,” Proc. - IEEE INFOCOM, no. ii, pp. 2074–2082, 2008.

[11] F. Anjum, D. Subhadrabandhu, and S. Sarkar, “Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols,” IEEE Veh. Technol. Conf., vol. 58, no. 3, pp. 2152–2156, 2003.

[12] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, “Intrusion detection for routing attacks in sensor networks,” Int. J. Distrib. Sens. Networks, vol. 2, no. 4, pp. 313–332, 2006.

[13] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, “WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks,” J. Sensors, vol. 2016, no. October, 2016.

[14] H. A. Babaeer and S. A. Al-Ahmadi, “Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking,” IEEE Access, vol. 8, pp. 92098–92109, 2020.

[15] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, “On the vital areas of intrusion detection systems in wireless sensor networks,” IEEE Commun. Surv. Tutorials, vol. 15, no. 3, pp. 1223–1237, 2013.

[16] Y. Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks,” Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM, vol. 1, no. 212, pp. 275–283, 2000.

[17] N. Chatterjee and J. K. Mandal, “Detection of Blackhole Behaviour Using Triangular Encryption in NS2,” Procedia Technol., vol. 10, pp. 524–529, 2013.

[18] I. E. Livieris and P. Pintelas, “A survey on algorithms for training artificial neural networks,” Dep. Math. Univ. Patras. Tech. Rep. TR08-01, 2008.

[19] A. A. Pirzada and C. McDonald, “Secure routing with the AODV protocol,” 2005 Asia-Pacific Conf. Commun., vol. 2005, no. October, pp. 57–61, 2005.

[20] S. Solanki and A. Gadwal, “Hybrid Security Using Digital Signature & RSA Encryption for AODV in MANET,” vol. 6, no. 3, pp. 2630–2635, 2015.

[21] M. G. Zapata, “Secure ad hoc on-demand distance vector routing,” ACM SIGMOBILE Mob. Comput. Commun. Rev., vol. 6, no. 3, pp. 106–107, 2002.

[22] T. Kullberg, “Performance of the Ad-hoc On-Demand Distance Vector Routing Protocol.”

[23] P. Manickam and T. G. Baskar, “Performance comparisons of routing protocols in mobile ad hoc networks,” vol. 3, no. 1, pp. 98–106, 2011.

[24] A. Lanjewar and N. Gupta, “Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocol,” Undefined, no. February, 2013.

[25] A. Syarif, E. E. Departement, U. Indonesia, K. B. Depok, and R. F. Sari, “Performance Analysis of AODV-UI Routing Protocol With Energy Consumption Improvement Under Mobility Models in Hybrid Ad hoc Network,” Int. J. Comput. Sci. Eng., vol. 3, no. 7, pp. 2904–2918, 2011.