Article

Not peer-reviewed version

Protecting AODV Protocol from Black Hole Attack in WSN

Sana AKOURMIS * , Youssef Fakhri , Moulay Driss Rahmani

Posted Date: 30 June 2023

doi: 10.20944/preprints202306.2186.v1

Keywords: Wireless Sensor Networks (WSNs); AODV; IDS (Intrusion Detection System); black hole attack; RREP (Route Reply) message; Security attack

Article

Protecting AODV Protocol from Black Hole Attack in WSN

Akourmis Sana [1,*], Fakhri Youssef [2] and Rahmani Moulay Driss [1]

[1] LRIT Laboratory, Faculty of Sciences, Mohammed V University in Rabat, Rabat B.P.1014, Morocco; d.rahmani@um5r.ac.ma

[2] LaRIT Laboratory Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco; fakhri@uit.ac.ma

* Correspondence: sana_akourmis@um5.ac.ma

Abstract: The development of wireless sensor networks (WSNs) technology comes with inherent limitations and vulnerabilities that make it exploitable by intruders. The fundamental goal of this article is to solve security problems related to black hole attacks, which interfere with the proper performance of the network and can lead to data leakage and loss. The proposed solution in this article is to apply IDS to a WSN for the first time. We also used the NS2.35 simulator to compare the three routing protocols, AODV, AODV under Hacker Node (HNAODV), and the proposed solution (IDSHNAODV) in the WSN model to reduce the effects of black hole attacks.

Keywords: wireless sensor networks (WSNs); AODV; IDS (intrusion detection system); black hole attack; RREP (route reply) message; security attack

1. Introduction

Wireless Sensor Network (WSN) is one of the new technologies that affects the world and our way of life and work since it requires wireless communication links instead of wires. WSNs have the possibility of sensing, processing, and communicating the signal to a base station (BS), which has applications in various fields. However, WSNs are vulnerable and permeable to the maliciousness of all kinds of attacks because of some security constraints that are a real security challenge to be faced, especially when the exchange concerns sensitive data that must reach the end-user [2]. A sensor node has five layers: the physical layer, the MAC layer, the link layer, and the application layer. Each one of these layers could be targeted by an intruder for specific purposes with a plan to eavesdrop on the WSN. So, it is necessary to minimize the risk of attack and transmit data to the end-user without being received in promiscuous mode [1,4]. Also, the nodes are resource-constrained [14,38], the WSNs have unique identification (ID), and they communicate with each other by the multi-hops mechanism. WSNs are exposed to acute security problems compared to wired mediums by being an open-air medium.

Security measures remain important in WSN to guarantee authentication, availability, confidentiality, privacy, no repudiation, anti-playback, and integrity [5]. We can conclude that they must have a certain level of security in order to effectively monitor where they are used and to ensure that the message and information are not altered during communication. So, data integrity is a mandatory operation that guarantees that the message does not alter, replay, or get spoofed during the transfer. The authentication of the message is still crucial in this situation since there is a chance that a hacker might access, rebroadcast, and edit messages, as well as even block the link to occupy the sensors. The integrity of the data is another aspect of this security method that is taken into consideration; each packet has a timestamp appended to it to ensure that no message is repeated. Additionally, data should be recent because, in such a network, shared data must come from reliable sources and is particularly sensitive. To prevent possible intruders from intercepting or reprogramming the content of signals shared by sensors, communication must be kept private and confidential. So that potential intruders are unable to intercept or reprogram the content of messages

shared by sensors. If not well protected, the network is at risk of going into promiscuous mode under malicious attacks [7]. This is the case with our attack, where the hacker node attracts the neighboring node using a higher sequence number, a false route reply, and fewer hops, and never broadcasts the received RREQ as it is required by the route discovery process. Various network layer attacks occur by modifying or adding some parameters of routing messages, such as the sequence number or hop-count. Such types of attacks are hard to detect. They always try to destroy or alter the information. Therefore, WSNs should include all three components of prevention, detection, and reaction to guard the system against collapse [2,6].

To fight attacks, many researchers have proposed various methods with a higher level of safety. despite the fact that each has a unique defense object and is unable to defend against a specific attack [25]. The WSN protocol should perform well in a variety of networking situations, from small ad hoc groups to larger mobile networks. Ad-hoc on-demand distance vector routing technology is used in WSN (AODV). His protocol encounters issues such as the Black Hole Attack, in which a malicious node sends a fake route reply message with a short and fresh route to the destination node using the highest sequence number because the utility of the sequence number is to determine the fresh route from source to destination, and it is a crucial attribute in routing. As a result, any information that attempts to contact the black hole node is unable to do so and is instead captured, resulting in low data and a significant end-to-end delay that we will address in the simulation section. It is crucial to examine how well the WSN defends against the Black Hole attack and how the network's implementation of an intrusion detection system (IDS) mechanism in the AODV routing protocol might help to lessen the impact of the attack. Applying IDS to a WSN for the first time is the suggested remedy in this article. The "recv Reply" function was used to determine whether or not the RREP message itself arrived. If so, the function indicates that the RREP message has already arrived by displaying it. If not, it executes the standard RREP function; if the RREP message was previously queued for the same destination address, it inserts the RREP message for that address and returns it from the function. Analyzing the WSN's performance against the Black Hole attack and how it could be avoided is crucial to better understanding how this solution operates. We presented our work at "IBICA'17".

This article will be divided into ten sections: in the first section, we will present the misbehavior mechanism in sensor networks, and then in Section 3, we will describe the existing threats in WSNs. Section 4 offers and discusses the related works of the proposed solution to counter this attack. The related works of the proposed solution to counter this attack. Section 5 presents an AODV protocol that behaves as the black hole nodes in NS2. We have simulated two scenarios, where each one has 25 nodes that use the AODV protocol. In addition, we will simulate the same scenarios after introducing from one to 5 nodes into the network as attackers. We will also present a solution to reduce the effects of these nodes in NS-2. Section 6 offers a detailed description of the different types of IDS for WSN, and in Section 7, the proposed algorithm presents an Intrusion Detection System based on the AODV protocol that is highlighted, especially the Blackhole attack, which is possible in most on-demand routing protocols, even secure ones, such as SAR (Secure-Aware Ad Hoc Routing protocol), ARAN (Authenticated Routing for Ad Hoc Networks), SAODV, SRP, ARIADNE, etc. [41]. The simulation environment and results are presented in Section 8 and studied and analyzed in Section 9. Finally, Section 10 concludes our paper.

2. Misbehavior Model for Wireless Sensor Networks

WSNs usually suffer from security attacks because of their features, such as the network's broadcasting character, wireless connectivity, environmental obstructions, transmission medium, lack of tamper-resistant packaging, cooperative algorithms, autonomous behavior of nodes, a collaboration between sensors, and the non-availability of network infrastructure. However, the main issue here is that when the network is exposed to certain conditions and situations, particularly in some cases, it is not the user manipulating it but rather a stranger who has access to the data. The question is, what does the attacker want from the targeted network? This question specifies the attack faced by the proper user (see Figure 1). Also, it may be due to the simplicity of the routing protocol

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

used to forward packets from one node to another, which is strictly required to maintain their connectivity over a wireless open medium in a distributed manner [9,39]. All these factors help attackers interrupt the network by, for example, transforming the routing protocol used to forward data to a central location (the "Sink") and interrupting network operations through mechanisms such as selective forwarding, data fabrication, or packet drops [37]. This will make other attacks against this specific form of ad hoc networking viable. Sensors are forced to interact with unpredictable environments where they may be subjected to a range of physical, biological, and chemical forces. Therefore, in the absence of wired networks, these networks must present specific security problems, and different management mechanisms must be implemented to increase their dependability. Because each attack has a unique defense mechanism, researchers must comprehend the many sorts of attacks and how they affect WSNs in order to guarantee secure communication and transmission [9].

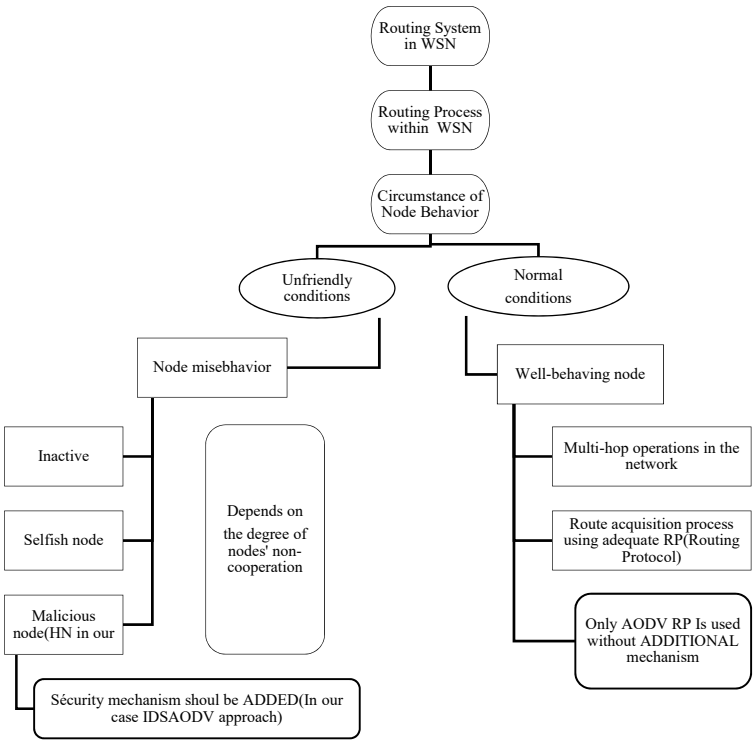

Figure 1. Summary of different node misbehavior in WSN [1,27,43,44].

Almost until now, all common routing protocols considered performance a priority and had little detection and defense ability against malicious nodes [28]. There are several types of routing protocols, including flat, data-centric, QoS-Based, geographical, multipath, and hierarchical routing. This classification is in Table 1. They are typically densely deployed (approximately 20 sensors/m^3), resulting in battery power waste due to the high mobility and density of sensor nodes. Consequently, WSN has high redundancy in sensing and communications, which creates collisions [8]. When nodes deplete their energy sensing and communicating the signal to the base station, data transmission consumes more energy than processing. Also, a long period between transmissions can occur. Finally, the most energy-consuming component is the R/F module, in which wireless communication is provided [39]. So, the ability to transmit data to the end-user while consuming less energy is the main objective of the routing protocol, and the network lifetime must be wisely prolonged. Finally, a good WSN design needs to be energy efficient to keep the network in its operating state to meet the needs of an application, without forgetting to mention that routing protocols are the key features of any network.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

Table 1. Routing-protocol classification in WSNs [6,12,19,22,23,30,31,33,38].

Routing Protocol Classification	Description	Examples of Protocols
Flat routing	It uses tremendously equal sensor nodes (in the case of processors, memory, and so on) that collaborate to sense the environment. All the nodes in the topology are assigned the same functionality or role.	AODV, DSDV, DSR, OLSR, PIN, Directed Diffusion (DD), SPEED, Rumor, MCFA, GBR.
Data-centric routing	The sink node usually asks for specific node data by broadcasting a message. When this message reaches the specific node where sink is interested in its data, the information will be returned to Sink. They depend on the name of the desired data. It eliminates many redundant transmissions.	SPIN, CADR, ACQUIRE, Rumor Routing, Gradient-Based Routing (GBR), Flooding, Gossiping, COUGAR, Directed diffusion Energy-Aware Routing.
QoS-Based routing	Routing is performed by applying QoS parameters, which usually control packet overhead and energy efficiency. A balance between energy consumption and data quality is maintained.	AODV, SAR, MLER, SPEED, GMCARE, MLER, MCBR, EAQSR, TBP, Maximum-lifetime energy routing; Maximum-lifetime data gathering; Minimum-cost forwarding; and an Energy-aware QoS routing protocol.
Location-based routing	It uses the location information of the node to forward data. In this case, overhead may significantly decrease. The routing path is decided according to the sensor nodes' position in the field.	MECN, SMECN, GAF (Geographic Adaptive Fidelity), GPSR; GPS (Global Positioning System), GEAR (Geographic and Energy-Aware Routing), GPSR, SAR.
Multipath-based routing	Multiple paths are used to enhance network performance, i.e., balance energy consumption, fault tolerance, energy efficiency, and reliability.	Maximum Lifetime Routing, DD
hierarchical routing	In hierarchical routing or cluster-based routing, the virtual tree is made by the nodes, and each node sends the packet to the base (the root of the tree) through the node. Nodes are assigned different roles or functionalities according to the hierarchy.	LEACH, PEGASIS, and Hierarchical-PEGASIS, TEEN, APTEEN, HEED, TTDD, MECN, HPEQ, Energy-aware routing for cluster-based sensor networks, Self-organizing protocol.

Among the challenges that routing faces in WSNs, two important issues are energy efficiency and security. Therefore, for the majority of current research in WSN, security methods and routing protocols are typically handled independently rather than built together [25]. Numerous researchers have proposed various safety protocols to guard against attacks. Each attack, however, has a unique set of countermeasures. Knowing what needs to be secured will be necessary to achieve security goals for sensor networks [39]. Routing protocols for wireless sensor networks should be as energy-efficient as possible to meet the needs of various applications. Since it is generally agreed that attacks cannot always be prevented or avoided, intrusion detection is needed as an additional line of defense. It is important to guarantee that the sensor network is protected from cyber-security threats. Also, detecting intrusions is the objective of Intrusion Detection Systems (IDSs), which already exist as a

tool for ensuring cybersecurity in traditional computer-based systems. IDSs can also offer additional mechanisms, such as prevention and diagnosis.

The fundamental characteristics are essential for the flexibility of WSNs. However, their vulnerabilities, such as insecure communication, broadcasting mechanisms, wireless connectivity, transmission medium, and sensor node dynamic behavior, make them vulnerable to a variety of attacks. So, specific security concerns that are absent in wired networks should be introduced in WSN [9]. Because of the simplicity of the routing protocol used to forward packets from one node to another, they must maintain distributed connectivity over a wireless open medium in a distributed manner [37,39]. Hence, the sensor node in the WSN is free to move independently in any direction.

Due to the scarcity of various resources that we have previously experienced, WSNs are vulnerable to a wide range of security assaults when an attacker or intrusive party manipulates vulnerabilities. Also, security mechanism do not prevent the misbehavior of sensor nodes because the wireless radios of these nodes are severely affected by these environmental factors [17]. And the communication faults that often occur in WSNs are due to interference. The attacker is affected by the possible paths that are selected by the sender to send data to the network and to take advantage of flaws in the routing protocol that are necessary for carrying out numerous attacks or gaining access to them. By doing this, they can drastically harm the topology of the network by rerouting data or interfering with routing protocols. It may compel nodes to overlook legitimate neighbor nodes or force them to mistakenly add neighbors that do not exist. Because all routes pass through a blackhole node that fails to establish a proper routing path between the source and destination nodes, attacks can target the OSI layers in the network stack [27]. And the effect of the attacker is greater if the attacker has more than one compromised node. Because a node may misbehave in a variety of ways, such as not transmitting data at all (black hole attack), forwarding data selectively, or going into sleep mode (snooze attack). This behavior of the intruder will influence the data reaching the base station and can affect the overall decision taken by the last user based on the collected data [5].

To sum up, the attackers always try to exhaust the energy of the sensor nodes. Also, attackers can use nodes with larger computing resources, such as laptops, to attack the nodes [24,37]. Laptop attacker nodes can communicate with sensors, introduce malicious code, and turn them into compromised nodes to violate their security mechanisms. These compromised nodes remain among the most damaging attacks on the WSN network. They can target a specific computer component, a certain network infrastructure, or an entire computer system, or even the entire internet infrastructure. As a result, each attack brings its own set of benefits and characteristics to the network [17]. To cover different classes of misbehavior, Figure 1 gives a global view of the network under both promiscuous mode and normal situations.

These attacks are classified into four categories: active, passive, external, and internal. In an active attack, the attacker exploits the weak link in the security protocol to initiate attacks like replaying, packet modification, DOS, spoofing, fabrication, node subversion, man-in-the-middle attacks, selective forwarding, etc. During a passive attack, the attacker obtains access to information like traffic monitoring, eavesdropping, and traffic analysis without being detected. These kinds of attacks are difficult to detect, and it is simply established by adversaries to intrude on network data exchange. Such attack recognition gets very hard since the network itself is not affected. In the case of an external attack on the network, the attacker is external and has no rights to access the network, including eavesdropping attacks, denial of service attacks, and resource exhaustion [10,28]. Finally, an internal attack occurs when it gets permission to access the network; the attacker, in this case, employs a malicious node to compromise the sensor nodes and take control of the network [12]. The attacker can use different plans to accomplish his malicious behavior on the network. So, it is challenging to find a general idea that can work efficiently for all kinds of attacks on WSNs [28]. In this regard, numerous threats [17] are described in this regard about a theory such as Gray Hole, Sybil, False or Malicious node, Flooding, Wormhole [26], Byzantine, Node capturing, Passive, Selective forwarding, Resource consumption, Location Disclosure Attack [1,4], and the Black Hole Attack, which is of interest in this paper. Once the type of attack is well understood, it provides an

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

idea of the best way to confront it because each attack has its own specific defense mechanism, as was mentioned before.

This study focuses on the Black hole attack that a hacker node conducts against the AODV routing protocol and the demonstrated mitigation method based on the RREP message on the AODV routing protocol. A summary of different attacks is shown in Table 2.

Table 2. Attack possibilities by OSI LAYER [5,12,13,24,26,28].

Attacks	Corresponding Layer
Denial of service (DoS), physical tampering, radio interference, physical capture, node, and interception.	Physical layer
Unfair attacks, energy depletion, Jamming, collisions, traffic manipulation, traffic analysis, monitoring, disruption MAC 802.11, WEP weakness, channel exhaustion, interrogation, unfairness, exhaustion, collision, and framing the conflict.	Data Link layer
Tampering with or sending false messages, modifying and replicating routing information, and disclosing information Gray-hole attack; sinkhole attack, hello flood attack, selective forwarding attack, Sybil attack, wormhole, and hello flood attack! Sending data to nodes out of transmission range, node capture, Spoofing, resource exhaustion, locator disclosure, homing, Byzantine, traffic analysis, and eavesdropping.	Network layer
Running out of memory, not synchronizing their attack, Session hijacking, packet injection attack, flooding., and port scan attack	Transport layer attack
Data gathering, task distribution, target tracking, repudiation, attacks on reliability, aggregation-based attacks, and DoS on the base station path due to overload Repudiation, data corruption, cloning, malicious nodes, SQL injection attack.	Application layer attacks

3. Related Works

Researchers propose numerous techniques and methods to detect and prevent black hole attacks in mobile ad hoc networks. In this regard, some of these works are presented below.

Deng, Li, and Agarwal [1] have proposed a mechanism to reject the route that contains the malicious node. Employing the route reply packet received from one of the intermediate nodes and the route request sent from the source node to a neighbor node to ensure that such a path exists from the intermediate node to the destination node. So, the source node S sends route request packets and receives a route reply through the intermediate node. However, if the intermediary node is a malicious node, the source node S will send Further Route Request packets to its neighbor node E to see if it has a routing list for this malicious node M. If not, node E is chosen as the new route to the destination. If not, node E is chosen as the new path to take in order to reach the desired location. This approach is effective only when there is a single attacker; it is ineffective when there are multiple attacker nodes and cannot identify a cooperative black hole assault.

An approach has been proposed in [5] by dynamically calculating a PEAK value after a fixed time interval by an intermediate node that uses three parameters for calculation: the routing table sequence number, the RREP sequence number, and the number of replies received at the time interval. This peak value is regarded as the highest value of a sequence number that any route response could possibly have at this time. The routing table marks the malicious node that sent the received RREP as one that should not be considered (DO_NOT_CONSIDER). Then, the received RREP is routed back to the source node through the reverse path. The advantage of this method is that no requirement is needed for any additional control packets added to the proposed Algorithm. In the same way, the malicious nodes are isolated, and the Packet Delivery Ratio (PDR) is improved considerably.

 doi:10.20944/preprints202306.2186.v1

Also, S. Ramaswamy et al. [8] have proposed an algorithm to prevent cooperative black hole attacks in ad hoc networks. It is based on establishing a trustful relationship between the nodes by introducing the Data Routing Information (DRI) table and cross-checking. The gray hole attacks cannot be tackled because of intensive cross-checking. This algorithm consumes more time to complete, even when the network is not under attack.

A watchdog-based method is developed in [11]. A node keeps copies of the watchdog-forwarded packets in a buffer to ensure that it sends packets properly. It is necessary to track the transmission of next-hop neighbors and identify problematic nodes to accomplish this. The overheard packet is compared with the one that is stored in the buffer, and if there is a match, the packet in the buffer is removed. Alternately, the watchdog increases the node's failure count, which is responsible for packet forwarding. The failure count surpasses a predetermined threshold when the node is identified as the misbehaving node and a notice is issued, message is delivered to the source node.

The passive overhearing-based watchdog method in [16] could only determine whether the next-hop neighbor sent packets. Otherwise, it is unable to determine the receiver's level of reception. The acknowledgment of packets forms the foundation of a scheme [18]. It is intended to address this problem. When a packet is sent by the source node, it waits for an acknowledgement packet from the destination node. Each node along the reverse route sends an acknowledgment back to the source node after the destination node has received a packet. An acknowledgment packet is successfully sent after the packet transmission. If not, a message of alarm is generated.

Z. Karakehayov [20] proposes a REWARD based on the routing algorithm to detect team black hole attacks in wireless sensor networks. In this method, the transmission of the sensor node performs power control for more than one sensor node in the direction of the BS through packet transmission. If a packet fails to forward an SN along the route, its neighbor will notice and report the SN as the black hole node in the next hop. REWARD uses geographic routing for forwarding. For its broadcast messages, the algorithm uses two different types; it brings together a dispersed database for identifying the SAMBA and MISS black hole attacks. MISS can help with the identification of malicious nodes working in the ID space. Likewise, SAMBA can provide the location of the detected black hole attacks related to the physical space.

The author [21] proposes ANB-AODV (Anti Near Black hole-AODV) to mitigate the impact of a black hole attack in MANET. So, when the source node broadcasts the RREQ packet, the first route reply will be from a malicious node to the source node, especially when this node is near the source node. Mostly, the source node will accept the first reply coming from the malicious node and start sending data packets. But when the second reply comes from the original destination after some time, it will accept the second reply and start sending through this alternative path. AFB-AODV (Anti-Far Black hole-AODV), the source node will accept the first reply that comes from the original destination node and reject the second reply. It has proposed a black hole attack approach that is effective for network performance. So, there is a decrease in packet loss when the ANB-AODV and AFB-AODV protocol are used. Furthermore, it improves the network's performance.

The author proposed a Secure Protocol for RElibled at a Delivery (SPREAD) in MANET in [15]. End-to-end delivery is intended. The secret-sharing technique breaks up shared data into smaller chunks and sends them over one or more independent pathways to their destination. As an alternative, dropping the single shortest channel for data routing between nodes is used. SPREAD performs better in terms of enhancing security. Its advantage is that it can withstand collusion attempts with more compromised nodes up to a certain number. The goals of multipath-based systems appear to be in conflict, particularly with regard to the quantity of information that must be redundant.

Another related study [29] put out the ERDA (Enhanced Route Discovery) method as a straightforward fix to eliminate misleading route entries. It requires less effort to mitigate the impact of blackhole attacks. Additionally, it functions without altering the current protocol scheme. This technique improves routing update functionality and separates malicious black hole nodes by analyzing received reply control messages (RREP). The blackhole feature is a high supported

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

destination sequence number in the route reply, and this technique assumes that the destination node is reachable via route request.

In [32], the authors have proposed the method DPRAODV (a dynamic learning system against black hole attacks in AODV- based MANET). The black hole node is prevented by informing other nodes in the network and setting a threshold. So, by sending the RREP sequence number (RREP_seq_no), we can check whether the sender is an attacker or not. If we consider that the value of (RREP_seq_no) is higher, the sender will be detected as an attacker and will be added to the blacklist. Then, it will be treated as the malicious node and ultimately will be blocked by not processing any of the RREP. The essential advantage of this protocol is; that the source node declares the blackhole to its neighbors as something to be ignored and removed. However, the cooperative black hole nodes are not supported by this method. Also, an overhead of updating threshold values at every time interval and the generation of the ALARM packet will significantly increase the routing even further.

4. Black Hole Attack in AODV

This section describes how the black hole attack might damage the AODV routing system. The three message types in AODV are RREP Packet, RREQ Packet, and RRER Packet. When a source node uses AODV as its routing protocol and has a packet to send, it first creates and broadcasts an RREQ packet throughout the network. The network is silent before this phase. RREQ continues transmitting in the network among the neighboring nodes until the destination node receives and accepts the packet. Along with the source address, this RREQ packet also includes a destination address and sequence number. When a link break is detected in any active route, the destination node responds by creating an RREP in the reverse path. The destination node in AODV uses the table Destination Sequence Number (DSN) to maintain each route entry [21]. It is generated by the destination when a connection is requested from it, and the route with the highest destination sequence number is designated for packet transmission. Also, the nodes check whether it has a direction to the destination, and the destination sequence number is used to identify the most recent path. The AODV protocol is one of the most distinctive among routing protocols as a result of this feature, but it lacks any security measures to prevent this active attack.

Meanwhile, when AODV is affected by this attack, a hacker node tends to provide false information about having the shortest route to the destination node to get all data packets, and all routing packets passing through it are dropped to interrupt regular communication. Also, all routes passing through it fail to establish a correct path between the source and destination node. This type of attack is an active DoS effective attack at the network layer and is far more vulnerable to attacks than any other layer in the WSN. In the following Figure 2, imagine a malicious node M. To communicate with the destination node, node S broadcasts an RREQ packet to its neighbor node which receives it. Nevertheless, node M is a malicious node that doesn't check its routing table for the requested route to node D. Thus, it immediately sends back an RREP, advertising the shortest path to the destination node. Node S chooses this route for packet forwarding and begins transmitting data packets to the destination node D as soon as it receives the RREP from node M presuming right away that this path through node M is the shortest. Since M is a malevolent node in the network, it acts like a black hole node by absorbing all the data and discarding it.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

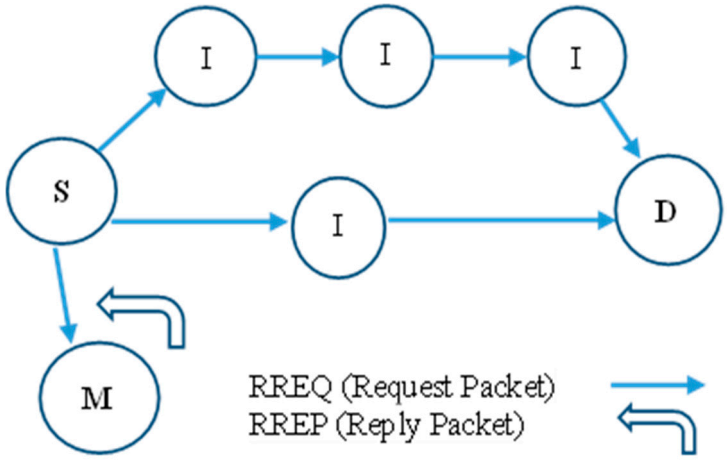

Figure 2. Black hole attack in AODV [21].

5. Summary of Ids in Wsn

Intrusion detection systems (IDSs) can identify both internal and external network threats in a sensor network. Unlike other security measures like cryptography which shields the network from outside attackers. IDS for sensor networks must notify the base station of any anomalies. However, because it is not practical to have an active, fully-powered agent within every node of a sensor network, the IDS solutions created for ad hoc networks cannot be used directly in sensor networks. Anomaly detection techniques can still be used to track these measures because their aim is still quite specific: to measure the physical data (such as sound or temperature) of its surroundings. Hence, both configuration protocols and hardware modules are highly specialized [42]. The nodes that originate from the actual world and adhere to specific parameters and patterns read all data. Creating a lightweight detection method for every protocol currently in use is a very challenging task due to the enormous number of protocols and packet formats that are given in the literature, especially in routing algorithms. At this level, we can see that node measurements are also vulnerable, and an adversary can try to influence this process for its benefit. However, there are partial solutions that enable a node to monitor the information exchange, confirm the integrity of the code inside a node, or test the status of a collection of nodes in order to determine whether they are alive or dead in order to verify the security of the sensor network. Although scheme may be incorporated into an intrusion detection system, no solution has been created particularly to interface with different schemes. Because of this, the IDS needs to be straightforward and highly tailored to the particular protocols used across the network and for responding to particular threats to sensor networks. Security is still required in this aspect to allow nodes to communicate securely in a potentially hostile environment. That has long been a hotly debated subject in wireless networks research. However, due to factors like limited resources and robust security measures, these cannot be introduced to avoid sensor node misbehavior as doing so would probably result in anomalous network operation.

The preventive mechanisms and security services, such as access controls, authentication services can improve the security of ad hoc networks. But they cannot deter all the possible insider attackers [35]. Especially when a denial-of-service (DOS) occurs, when an entity cannot execute an action or access a service that it is entitled to. That's why the foremost task of the sensor node is to analyze environmental data, and an adversary can try to influence this process for its benefit. Hence, all data is read by the nodes that come from the real world and respect determined patterns and limits [36]. Thus, it is necessary to have other security mechanisms to treat misbehaving insider nodes which possess access rights. The majority of these measurements may be monitored using anomaly detection techniques. Any change in the accelerometer's readings suggests that the node is stolen by an unauthorized party, and an alarm will sound. Additionally, the local agent keeps an eye on packets are sent directly to the node. Also, if a node takes a long time to send a packet because the channel is unavailable. Misuse techniques can be used to locate an abnormal situation that necessitates raising an alarm. The local agents are there to look for threats or attacks that might interfere with the sensor

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

nodes' typical operation. This can be accomplished by focusing solely on local data sources, such as the node's real status, packets it broadcasts and receives, all of its neighbors' known information, and environmental measurements [42]. But those attacks must be recognized by the local agency. In a nutshell, the security measure should guard against both external and internal system intrusions. Because this last relies on the collective protection of all nodes and in particular lacks centralized monitoring in a wireless sensor network and management points, it should not be for a single layer in the network but should instead protect each node [35,36].

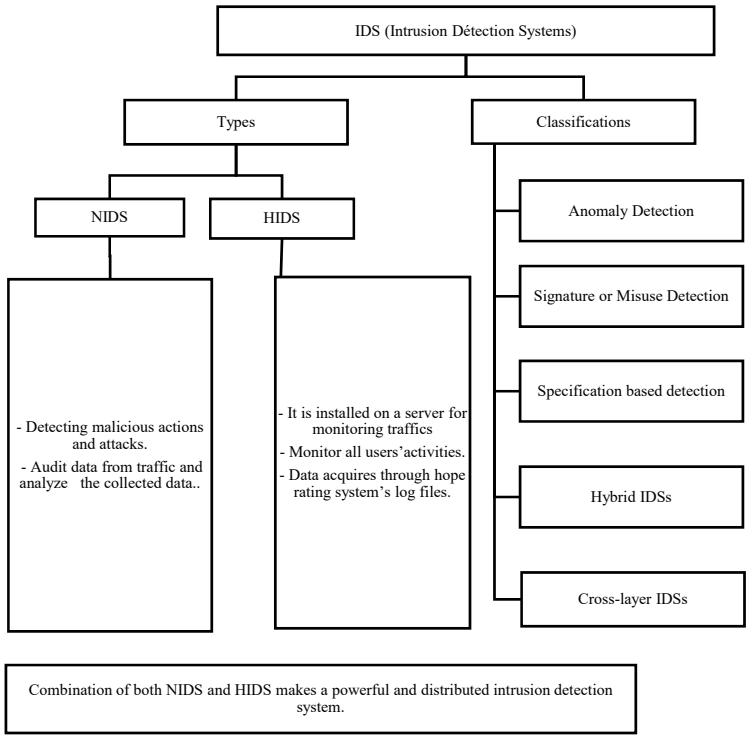

Figure 3. Classification and types of IDS [35,36,40].

6. Algorithm AODV-IDV

This mechanism assumes the destination node is accessible by route request, and the usual black hole characteristic is the high destination sequence number supported in the route reply. This sequence number is used to determine the raw route from the source to the destination. Also, SN (the source node) indicates that it has the shortest path to the destination. The solution here is based on the Intrusion Detection System (IDS) that treats the first RREP (Route Reply) coming from the black hole node by analyzing its sequence number in this RREP packet if it is higher than the sequence number at the source. In this case, the node that sent this RREP packet is considered a malicious node in the AODV (Ad hoc on Demand Distance Vector) network. AODV borrows the concept of "destination sequence numbers" from DSDV for maintaining the most recent routing information between nodes. Otherwise, the nodes do not have to maintain and discover a route to another node until they need to communicate. But the former node is offering its services as an intermediate forwarding station to maintain connectivity between other nodes. A hacker node or sequence number attack is one of the active attacks that occur in the network's routing by sending fake route reply messages and announcing them as having the shortest path to the destination node. The other nodes will trust it by choosing its path, and they will start receiving all the data packets from neighbors' nodes and then drop all the received packets, delaying or blocking communication in the networks. We attempt to use this solution to focus on analyzing and improving the security of the AODV (Ad hoc On-Demand Distance Vector) routing protocol and how IDS implementation contributes to securing WSN against this attack, especially in terms of packet loss and transmission delay reduction.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

The routing table contains information about the path to a destination because every node in an ad hoc network maintains it. As a result, the attacker has an impact on every route that could be used by the sender to deliver data over the network. The information obtained from the attacker via the DSN identifies this claim. We had to change the RREP function (recv Reply) and create an RREP caching mechanism to count the second RREP message in order to implement the solution. For this purpose, this algorithm is implemented by changing the normal receive RREP function (recv Reply) and replacing it with a RREP caching mechanism to count the second RREP message. In the "recv Reply" function, we first check if the RREP message has arrived for itself, and if it has, the display function of the RREP message if it has already arrived. If this is not the case, it inserts the RREP message for its destination address. Also, if the RREP message is cached previously for the same destination address, the normal RREP function is performed. Subsequently, if the RREP message is not destined for itself, the node transmits the message to its appropriate neighbor. Besides, there are four sub-functions added to the RREP caching mechanism, namely, "rrep_insert", "rrep_lookup", "rrep_remove", and "rrep_purge" and each sub-function has its own role, as mentioned in Figure 5, to prevent the first or second RREP from coming from the black hole node. The meaning of each sub-function is given in Figure 4.

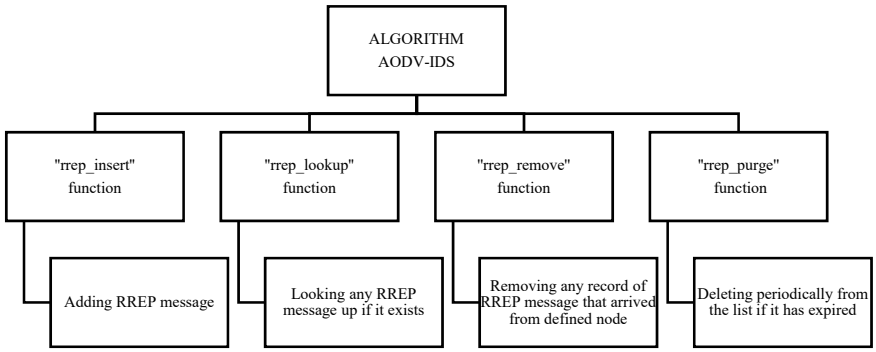

Figure 4. The operating system of IDS-AODV.

In the following flowchart (Figure 4 [9]), the mechanism of this technique is presented.

The blackhole node typically does not check the routing database for acceptable routing options as it would in typical cases because it generates an instantaneous response. Because of this, the false node, which is the malicious node, participates in the network with the high destination sequence number, but the malicious node or the genuine destination node will send the first route reply. The latter may be saved in the RR-Table's entry.

The IDSHNAODV algorithms will discard this first RREP packet from the malicious node and choose the second RREP packet from the destination, ultimately finding another path to the destination. Last but not least, it compares the first destination sequence number with the source node sequence number, and the node is malicious if there are more differences between them. As a result, remove that entry from the RR-Table.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

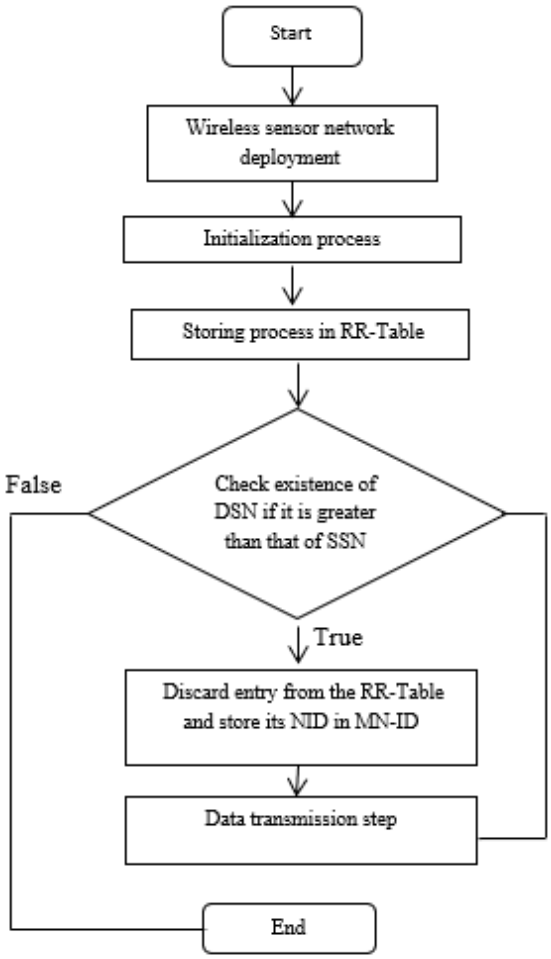

Figure 5. Flowchart of the existing algorithm [9].

7. Proposed Algorithm for Intrusion Detection System with Wsn

WSNs are considered to be highly vulnerable and easily attacked by malicious actions. In this present section, an overview that is purely based on our experience will be given. The First attempt presents three instances of the AODV protocols, namely: in the normal situation, under attack, and with the IDS solution. The latter tries to change the route response coming from the BH node. To begin, in a normal situation, we configure the attack to be absent from all nodes in the WSN architecture, as shown in procedure 1 below. Hence, the transmission and reception of messages through AODV are done in a non- adversarial environment. In procedure2, we have made the network an in-adversarial environment by creating a black hole. Because there were hackers on WSN at that time, AODV's dependability and network performance suffered. The attacker's influence and potential, as well as that of the layer in question, will all be considered as part of this current endeavor. The suggested intrusion detection system monitors the initial RouteReply that the hacker node sends before contacting the source node, which determines the route that should be taken to get to the intended destination. However, the initial RouteReply that the source node sends is the one that was initiated by the hacker node. That is caused by a forgotten message that answers all RREQs most concisely. In the proposed IDS, as shown in procedure 3, the first route reply is checked at the source node to see if it has already arrived by itself, especially since the hacker node responds to all RREQ with the same route reply within a short period of time. Occasionally, this response is captured. In a nutshell, the IDS-AODV protocol will discard the first RREP packet from BH/attacker node and choose the second RREP packet from the destination. Consequently, the IDS-AODV Protocol will also find another route to its destination.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

Procedure1: Creation of WSN Architecture

```
# Nodes Definition
#Create 25 nodes
for {set I 2} {$i< $val(nn) } { incr I }
{
        set node_($i) [$ns node]
        $node_($i) set X_ [expr { rand()*800} ]
        $node_($i) set Y_ [expr { rand()*550} ]
        $node_($i) set Z_ 0.0
        $ns initial_node_pos $node_($i) 25
}
```

Procedure2: Setting two nodes as hackers

```
# declaring a node as hacker or attacker
#Setting node 0 as attacker
$ns at 0.0 "[$node_(0) set ragent_] hacker"
#label- indicating it is a black hole attacker
#A hacker node drops and discards all    # received messages
$node_(0) color red
$ns at 0.0 "$node_(0) color red"
$ns at 0.0 "$node_(0) label Attacker"
# source, destination, and attacker nodes are declared from 1 to25
```

Procedure3: Proposed Detection System IDS-AODV against Malicious Node (MN)

```
# Set the waiting time (WT) to receive the RREQ coming from other nodes
#then add the current _time to the waiting _time
#in the storage process, it stores all the #RREQ(DSN)Destination Sequence Number
#and the NID is stored in the RR-#Table as its node id in until the time expires.
# in the "Prior Receive Reply" method
If((Dst_Seq)>( Dst_Seq at the Source))
Then The send node"RREP packet"= Attacker
Not a legitimate_Node
If ( (RREP_message)= (Arrived_for_itself at the Source ))
Then Choose another Path to Dst
RREPCaching mechanism    modifies RREP function
```

8. Simulation Environment

The research done to compare the performance of the AODV routing protocol in the WSN network and under the IDS approach when the attack is active has been detailed in this section. The performance of the AODV routing protocol is analyzed against parameters like packet loss, average throughput in kbps, energy in joules, and end-to-end delay under various scenarios using NS-2(v-2.35). In our simulation, 25 nodes were allowed to move in an 800x550 m rectangular region for a 200 s simulation. We obtained the initial locations of the nodes using a uniform distribution. The "Random way-point" model is adopted to simulate node movement. Simulations are running with 10 seeds. The chosen parameters for simulation are presented in Table 3.

Table 3. Experimental Setup.

Simulation Time	**200.0 sec**
Topology	Mobile
Node Placement	Random

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

Terrain Dimension	800 x 550
Antenna Model	Omni Antenna
Number of Nodes	5, 10,15, 20,25
MAC Layer	802.11
Routing Protocols	AODV, BLACK HOLE AODV, and IDS AODV
Radio Propagation Model	TwoRayGround
Traffic Model	Constant Bit Rate
Packet Size	256
Traffic Rate	0.1 mbps
Number of malicious nodes	0 to 10
Transmission range	250 m
Observation parameters	PDF, end-to-end delay, throughput, and energy

9. Results & Discussion

A simulation study has conducted to evaluate the performance of WSN in the presence of attacks using metrics such as packet loss, throughput, end-to-end delay, and average energy. The results in Figure 3 show the presence of five attackers. And the IDS approach has also been used in the presence of a black hole attacker node to check the network 's performance. Initially, we measure packet loss, throughput, delay, and energy by varying the number of nodes. So, we fix the number of malicious nodes to 4 (see Figure 7). For the rest of the graphs, we have set the number of malicious nodes to one for the sake of comparison between AODV, AODV under black hole attack (HNAODV), and IDS when this attack is active. The black hole node is chosen randomly in the simulation test and increases the delay in the network. The simulation results are shown in Figures 8–12, which show the network throughput, average delay, average energy, and packet loss without and with both an attack and an IDS approach, respectively:

AODV drops more packets under malicious attacks compared to normal AODV under a varying number of communicating nodes (see Figure 6). It is concluded that conventional AODV (without malicious attacks) has fewer packets to lose in comparison to AODV with malicious attacks because the node under attack does not permit additional packets to flow to their surrounding nodes. With more malicious nodes dropping more packets, AODV experiences greater packet loss. And it doesn't authorize the packet to flow further; it occurs because the number of packets delivered greatly decreases as all packets traversed in the attacker's path will be dropped and absorbed through it. It is so because the intruder has to disable the sender by not broadcasting the RREQ that is received from intermediate nodes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

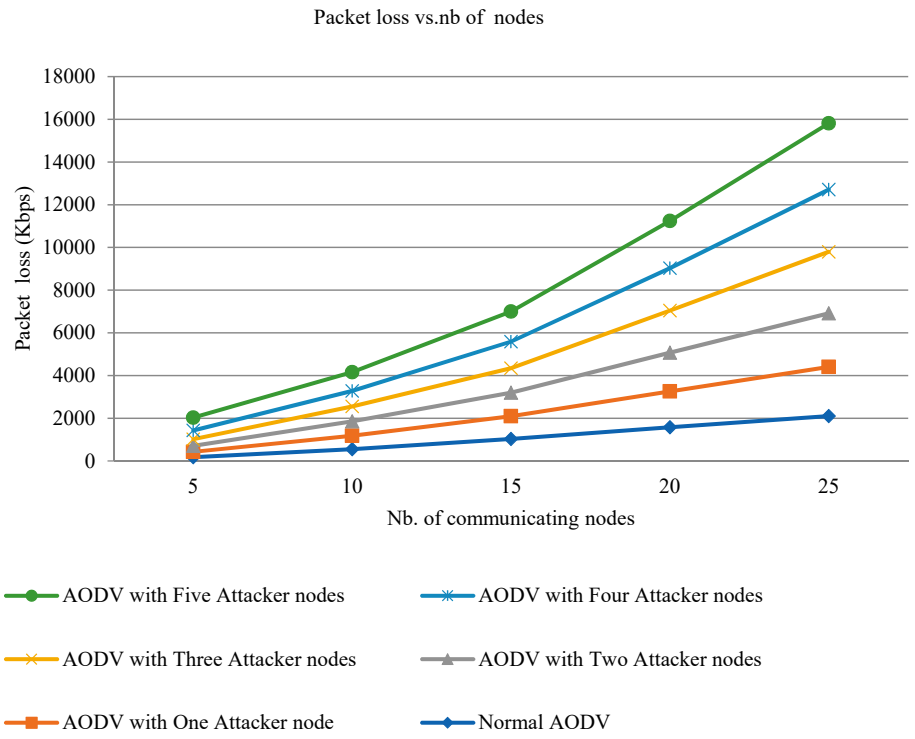

Figure 6. Packet loss vs. number of nodes.

Table 4. The impact OF HACKERS ON AODV PACKAGE LOSS.

Number of Hackers on Nodes (Attackers)	Packet Loss on AODV (%)
1	8
2	15
3	22
4	25
5	34

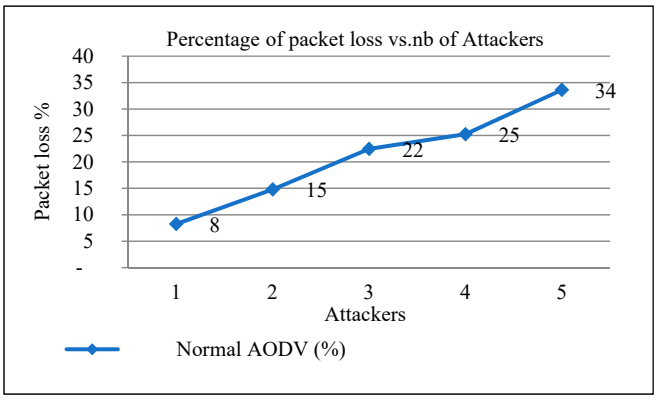

Figure 7. Packet loss vs. number of nodes.

From Figure 7, we deduce the increasing number of packet losses when the number of attackers increases.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

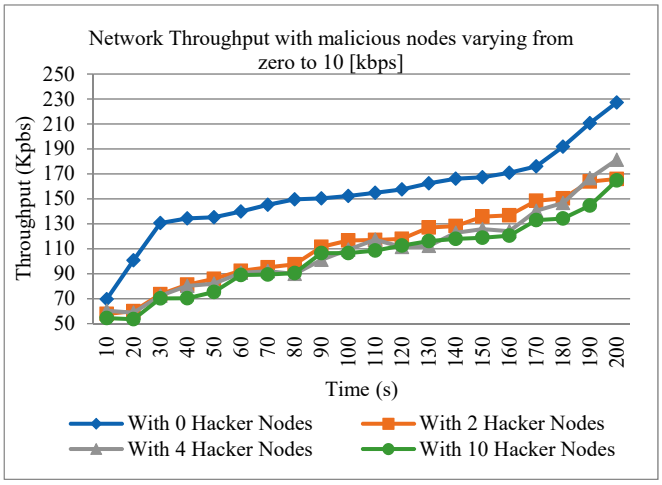

Figure 8. Network throughput under malicious behavior.

According to Figure 8, as the number of malicious nodes increases, throughput will decrease.

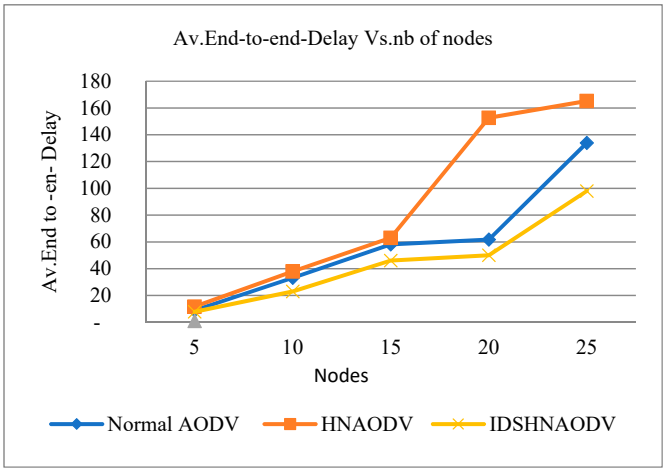

Figure 9. Average End-to-End Delay vs. number of nodes.

First, in the absence of an attack graph, it sends bits from the source to the destination node. Following that, we introduce one false node into the network; this false node is the black hole (a natural hacker). Then network latency occurs (see Figure 9).

From Figure 9, (IDSHNAODV) shows a low delay compared to AODV, and for AODV under a black hole attack, it will be increased with the increased number of nodes. Also, all nodes are movable, and the topology of the network is dynamically changing in a WSN network, which presents great challenges to the security of the wireless sensor network. As a result, any data that enters the black hole region is captured and is not able to attain its destination, which causes high end-to-end delay and low throughput. According to Figure 10, adding malicious nodes causes the routing protocol (AODV) to perform worse. This is especially true as the number of nodes grows because the malicious assault will reduce throughput (see Figure 8). As a result, attackers may alter node behavior, changing the outcomes

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

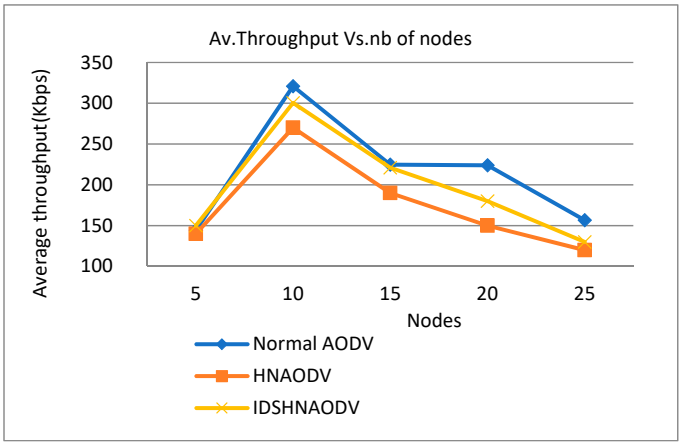

Figure 10. Throughput vs. number of nodes.

Figure 10 indicates that the throughput of the AODV routing protocol increases as long as the number of communicating nodes increases. But with malicious attacks, the throughput of AODV is lower compared to normal AODV. Throughput calculates the network's performance in normal conditions, in the presence of a black hole attack, and in the presence of an IDS to enhance the network's performance. And it shows the throughput results of Ad-hoc On-demand Distance Vector (AODV), AODV under one hacker node, and (IDSHNAODV) with the attack.

It is clear from the graph that we observe a significant improvement in throughput results for (AODV), and (IDSHNAODV) under the black hole node for a 10 nodes scenario compared to only AODV under the attacker (HNAODV). As the number of nodes increases, throughput decreases.

It is clear from Figure 11 that energy consumption is proportional to the number of nodes. Therefore, when the number of nodes increases, energy consumption decreases automatically for all protocols: (AODV), (HNAODV), and (IDSHNAODV). All protocols will have similar energy because adding a few tasks like IDS to a node won't reduce its energy a lot. On the contrary, it should be negligible.

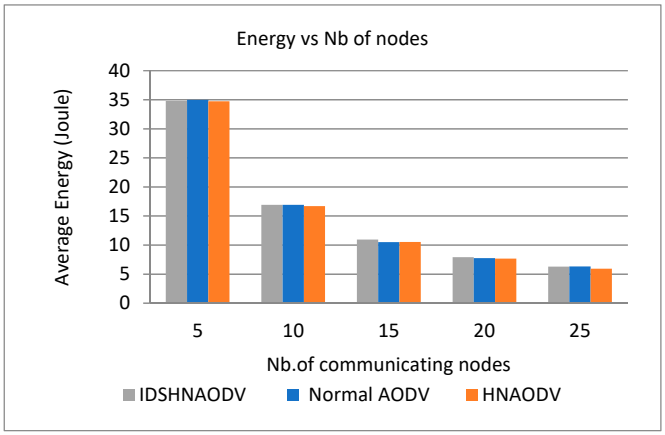

Figure 11. Energy vs. number of nodes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2023 doi:10.20944/preprints202306.2186.v1

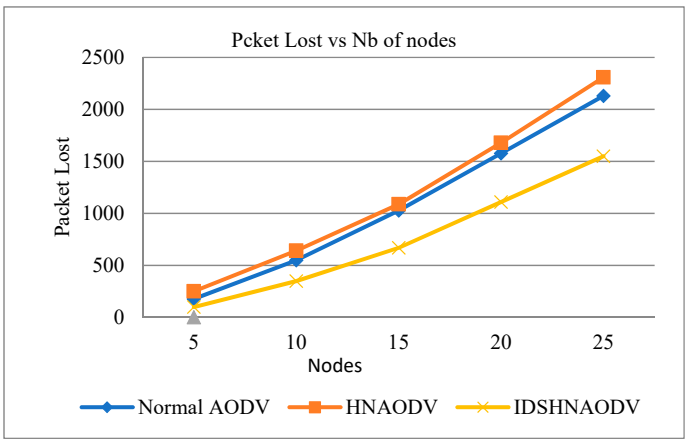

Figure 12. Packet loss vs. number of nodes.

According to Figure 12, normal AODV (in the absence of an attack) has less packet loss than AODV with a malicious attack because nodes do not allow more packets to pass to neighboring nodes when under attack. Then, we have measured the packet drop of AODV with Black hole under the IDS approach, and in this case, packet loss increases. It is clear from the graph that the hacker node produced by the black hole attack affects the performance of routing by dropping the data packets in the network. Once, the route is established through that node, the neighboring node starts sending packets, which eventually will be dropped at the adversary. Therefore, as the number of malicious nodes increases, their effect increases further. AODV drops more packets under malicious attacks compared to normal under a varying number of communicating nodes (see Figure 12). Finally, the increased number of attackers will affect the performance of all metrics on the network.

10. Conclusions

In this paper, we have analyzed the impacts of the black hole attack on an AODV network. We have implemented an AODV protocol that acts as a black hole (HNAODV) in the NS-2 simulator. We have simulated five scenarios with 25 nodes, and for each scenario, we have created one to five malicious nodes in the network and studied their impact on network performance. The simulation results have shown that under black hole attack, an essential part of packets is rejected, and packet delay becomes unacceptable. We have determined how malicious nodes are dropping as a result of the blackhole attack, data packets and blocking communication between source nodes and destinations. We have implemented the IDS solution we have adopted and tested this slightly modified version of the AODV protocol in a WSN model to observe how it has contributed to reducing the black hole effects. It is concluded that by introducing malicious nodes, the performance of the routing protocol (AODV) degrades under the black hole attack while throughput increases. Based on results obtained from simulation, the IDSHNAODV solution can reduce the packet drop in the network significantly and is capable of reducing the impact of the black hole attack in the sensor network. The advantage of using this approach is that IDSHNAODV has minimal modifications to the AODV protocol, does not require any additional overhead, and does not require any modifications to the packet format during implementation. In the future, we will investigate other types of network layer attacks, such as a gray hole or wormhole attack on the standard AODV protocol, and we will try to study how we can reduce the effect of these attacks on the network, either by testing the same technique or by introducing another response system to keep network performances at acceptable and desired levels.

References

1. Sharma, Kalpana, and M. K. Ghose. “Wireless sensor networks: An overview on its security threats.” IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs (2010): 42-45
2. Modirkhazeni, Ali, NorafidaIthnin, and Othman Ibrahim. “Empirical Study on Secure Routing Protocols in Wireless Sensor Networks.” Int. J. Adv. Comp. Techn. 2.5 (2010): 25-41.

3. H. Deng, W. Li, and D. P. Agrawal. "Routing Security in Adhoc Networks." In: IEEE Communications Magazine, Vol. 40, No. 10, pp. 70-75, Oct. 2002.
4. Dokurer, Semih. Simulation of Black hole attack in wireless Ad-hoc networks. Ankara: Atılım University, 2006.
5. Didla, S., Ault, A., &Bagchi, S. (2008, March). Optimizing AES for embedded devices and wireless sensor networks. In Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities (p. 4). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
6. Sana Akourmis, Youssef Fakhri and MoulayDrissRahmani"REDUCING BLACK HOLE EFFECT IN WSN " IBICA'17 ,the 8th International Conference on Innovations in Bio-Inspired Computing and Applications,Marrakech, Morocco,December 11-13, 2017
7. Chelli, K. (2015, July). Security issues in wireless sensor networks: attacks and countermeasures. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 1-3).
8. Singh, Kuldeep, and Sudesh Rani. "A performance study of various security attacks on aodv routing protocol in manet." International Journal of Computer Applications 101.14 (2014).
9. Renold, A. P., Poongothai, R., &Parthasarathy, R. (2012, January). Performance analysis of LEACH with gray hole attack in Wireless Sensor Networks. In Computer Communication and Informatics (ICCCI), 2012 International Conference on (pp. 1-4). IEEE.
10. Chen, X., Makki, K., Yen, K., &Pissinou, N. (2009). Sensor network security: a survey. IEEE Communications Surveys & Tutorials, 11(2).
11. Maidamwar, Priya, and NekitaChavhan. "Impact of wormhole attack on performance of LEACH in wireless sensor networks." International Journal of Computer Networking, Wireless and Mobile Communications 3.3 (2013): 21-32.
12. Lou, W., Liu, W., & Fang, Y. (2004, March). SPREAD: Enhancing data confidentiality in mobile ad hoc networks. In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies (Vol. 4, pp. 2404-2413). IEEE.
13. Vyas, T. G., and D. J. Rana. "Survey on black hole detection and prevention in MANET." IJARCSSE4 (9),(September 2014) (2014).
14. Rao, RayalaUpendar. "Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys." International Journal of Computer Applications 55.7 (2012).
15. Shankar, M., Sridar, M., &Rajani, M. (2012). Performance evaluation of LEACH protocol in wireless network. International Journal of Scientific & Engineering Research, 3(1), 1.
16. Karakehayov, Z. (2005). Using REWARD to detect team black-hole attacks in wireless sensor networks. Wksp. Real-World Wireless Sensor Networks, 20-21.
17. Gurung, S., &Saluja, K. K. (2014). Mitigating impact of Black hole attack in MANET. In Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC.
18. Frey, H., Rührup, S., &Stojmenović, I. (2009). Routing in wireless sensor networks. In Guide to Wireless Sensor Networks(pp. 81-111). Springer, London.
19. Patil, M., &Biradar, R. C. (2012, December). A survey on routing protocols in wireless sensor networks. In Networks (ICON), 2012 18th IEEE International Conference on (pp. 86-91). IEEE.
20. Suryawanshi, Ranjeet, and Sunil Tamhankar. "Performance Analysis and Minimization of Black hole Attack in MANET." International Journal of Engineering Research and Applications (IJERA), ISSN (2012): 2248-9622.
21. Ferng, H. W., &Rachmarini, D. (2012, April). A secure routing protocol for wireless sensor networks with consideration of energy efficiency. In Network Operations and Management Symposium (NOMS), 2012 IEEE (pp. 105-112). IEEE.
22. Maidamwar, P., &Chavhan, N. (2013). Impact of wormhole attack on performance of LEACH in wireless sensor networks. International Journal of Computer Networking, Wireless and Mobile Communications, 3(3), 21-32.
23. Gorlatova, M. A., Mason, P. C., Wang, M., Lamont, L., &Liscano, R. (2006, October). Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis. In Military Communications Conference, 2006. MILCOM 2006. IEEE (pp. 1-7). IEEE.
24. Sana, Akourmis, Fakhri Youssef, and RahmaniMoulayDriss. "FLOODING ATTACK ON AODV IN WSN." 2018 Renewable Energies, Power Systems & Green Inclusive Economy (REPS-GIE). IEEE, 2018.
25. Jali, K. A., Ahmad, Z., & Ab Manan, J. L. (2011). Mitigation of black hole attacks for aodv routing protocol. International Journal of New Computer Architectures and their Applications (IJNCAA), 1(2), 336-343.
26. Renold, A. P., Poongothai, R., &Parthasarathy, R. (2012, January). Performance analysis of LEACH with gray hole attack in Wireless Sensor Networks. In Computer Communication and Informatics (ICCCI), 2012 International Conference on (pp. 1-4). IEEE.

27. Naik, A. S., &Murugan, R. (2018). Security Attacks and Energy Efficiency in Wireless Sensor Networks: A Survey. International Journal of Applied Engineering Research, 13(1), 107-112.
28. Raj, P. N., &Swadas, P. B. (2009). Dpraodv: A dyanamic learning system against Black hole attack in aodv based manet. arXiv preprint arXiv:0909.2371.
29. Boukerche, A., Pazzi, R. W. N., & Araujo, R. B. (2005, November). Hpeq a hierarchical periodic, event-driven and query-based wireless sensor network protocol. In Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on (pp. 560-567). IEEE.
30. Maidamwar, P., &Chavhan, N. (2013). Impact of wormhole attack on performance of LEACH in wireless sensor networks. International Journal of Computer Networking, Wireless and Mobile Communications, 3(3), 21-32.
31. Sasikala, S., &Vallinayagam, M. Secured intrusion detection system in mobile ad hoc network using RAODV. Proceedings published in International Journal of Computer Applications (IJCA), ISSN, 975, 8887.
32. ECE, S. B., & ECE, L. Analysis of Black Hole Effect and Prevention through IDS in MANET.
33. Almomani, I., Al-Kasasbeh, B., & Al-Akhras, M. (2016). WSN-DS: a Dataset for intrusion detection systems in wireless sensor networks. Journal of Sensors, 2016.
34. Zaman, N., Tang Jung, L., &Yasin, M. M. (2016). Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol. Journal of Sensors, 2016.
35. Jung, J., Cho, Y., & Hong, J. (2012). Impact of mobility on routing energy consumption in mobile sensor networks. International Journal of Distributed Sensor Networks, 8(3), 430439.
36. Khan, S., Lloret, J., & Loo, J. (2014). Intrusion detection and security mechanisms for wireless sensor networks.
37. Pal, R., Azad, M., & Kumar, S. (2013). An Approach to Combat the Black hole Attack in AODV Routing Protocol. International Journal of Computer Applications, 77(11), 13-19.
38. Roman, R., Zhou, J., & Lopez, J. (2006). Applying intrusion detection systems to wireless sensor networks. In IEEE Consumer Communications& Networking Conference (CCNC 2006).
39. Mamatha, G. S., and Dr SC Sharma. "Network layer attacks and defense mechanisms in MANETS-a survey." International Journal of Computer Applications 9.9 (2010): 12-17..
40. Culpepper, B. J., & Tseng, H. C. (2004, October). Sinkhole intrusion indicators in DSR MANETs. In First International Conference on Broadband Networks (pp. 681-688). IEEE.
41. Akourmis, S., Fakhri, Y., &Rahmani, M. D. (2020). Design Model and Deployment Fashion of Wireless Sensor Networks. In Wireless Sensor Networks-Design, Deployment and Applications. IntechOpen.
42. Hollick, M., Schmitt, J., Seipl, C., & Steinmetz, R. (2004, June). On the effect of node misbehavior in ad hoc networks. In 2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577) (Vol. 6, pp. 3759-3763). IEEE.
43. Hollick, M., Schmitt, J. B., Seipl, C., & Steinmetz, R. (2004, February). The ad hoc on-demand distance vector protocol: an analytical model of the route acquisition process. In *International Conference on Wired/Wireless Internet Communications* (pp. 201-212). Springer, Berlin, Heidelberg.