PERFORMANCE EVALUATION OF WIRELESS SENSOR NETWORK IN PRESENCE OF GRAYHOLE ATTACK

Adnan Ahmed*, Muhammad Ibrahim Channa**, Umair Ali Khan*

ABSTRACT

The tremendous growth in wireless communication and digital electronics has led to the development of low-cost and low-power sensor nodes that are small in size and may communicate over short distances. Sensor nodes are deployed in hostile environment in large number, which makes their physical protection against tampering difficult or more prone to be compromised by an adversary force. By doing that, an adversary can modify the behavior of the compromised nodes and launch routing misbehavior attacks. One most common type of such attacks is grayhole attack. Adhoc On Demand Distance Vector (AODV) in its pure form does not have any mechanism to deal with such type of attack. In this paper, we simulate grayhole attack on AODV routing protocol and evaluate AODV's performance by considering different metrics and scenarios. NS2 simulator has been used to conduct simulation of grayhole attack. Our simulation results show the influence of grayhole attack on the performance of AODV which suffers from decreased delivery ratio and increased packet loss. Furthermore, some countermeasures against grayhole attack are also provided.

Keywords: Wireless sensor networks; grayhole attack; security; node misbehavior; blackhole attack; AODV

1. INTRODUCTION

Sensor networks are the type of wireless network that consist of large number of tiny sensor nodes and base stations having sensing, data processing and communicating capabilities. The sensing unit collects data about some physical phenomena such as light, sound, vibration, humidity, temperature and heat [1]. WSN may have useful applications for both civilian and military. Civilian applications of sensor networks include building automation, smart environments, monitoring the status of structures (such as bridges), robot control and guidance in automatic manufacturing environments, factory process control and automation, vehicle tracking and detection, monitoring disaster area, increasing the effectiveness of agricultural processes and water management, environmental monitoring, and health monitoring (to name a few). In the military applications, WSN can be used for surveillance, battle field monitoring, monitoring equipment and ammunition, battle damage assessment, targeting, and reconnaissance [2].

Security is a major challenging issue in wireless sensor networks applications because they are operated in public and unrestrained areas. The foremost goal of providing security is to protect the network resources against a number of attacks such as DoS attack, wormhole attack, blackhole attack, grayhole attack, routing table overflow attack, packet replication attack, and modification of packets attack [3–6]. This unattended nature of WSN makes sensor nodes vulnerable to various types of attacks such as node physical capture, selfish and malicious behavior of nodes. In this study, we address a common type of node misbehavior caused by grayhole attack. The node misbehavior caused by grayhole attack is similar to blackhole attack to some extent. However, in contrast to blackhole attack, a node under grayhole attack drops packets selectively rather than dropping all the received packets [7]. The node misbehavior issues such as blackhole and grayhole [8] are popular security threats in WSN and many researchers have proposed solutions to counter these attacks. Nevertheless, no generic and unconstrained solution exists to prevent such attacks completely [9].

In this paper, our methodology is to discuss how grayhole nodes makes use of AODV routing process and yield attack in routing packets. The performance of sensor network in the presence of several grayhole nodes is also compared. Most of the existing literature on performance evaluation of grayhole attack does not addresses the impact of an attack on a node's energy, as it is important design parameter for energy constraints

* Assistant Professor, Department of Computer System Engineering, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, Pakistan

** Professor, Department of Information Technology, Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, Pakistan

network, specially WSN. Furthermore, some counter-measures against grayhole attack are also provided. The rest of the paper is organized as follows. Section 2 briefly provides the overview of AODV routing protocol and discusses the related work in this domain. Section 3 explains the grayhole attack mechanism and the algorithm for launching a grayhole attack. Section 4 gives the simulation model of grayhole attack. Section 5 presents the simulation results of grayhole attack with our analysis. Section 6 provides countermeasure mechanisms against grayhole attack. Section 7 concludes the paper with some potential future work.

2. AODV PROTOCOL AND THE RELATED WORK

Adhoc On Demand Distance Vector (AODV) [10] is an on-demand routing protocol that creates routes between a source and a destination on the fly (upon request by source node). AODV provides fresh enough routes and is more scalable. Two important control packets, Route Request (RREQ) and Route Reply (RREP), are used to discover a route. The process of discovering a route is shown in Figure 1.

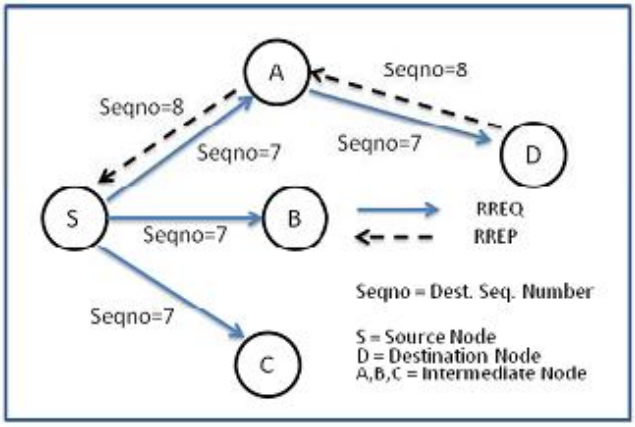

Fig. 1: AODV route discovery mechanism

RREQ and RREP contain some important attributes such as destination sequence number and hop count, which help in determining the freshness of the route. Both of these values are incremental values. Source node (node S) broadcasts the RREQ packet to all of its reachable neighbors (A, B and C) whenever it needs to establish a route with the destination. Upon reception of RREQ packet, either of the following task(s) is performed by the neighboring node(s):

i. The intermediate node responds with RREP packet to source node if it is the destination node or the node may have "*fresh route*" information to destination.

ii. The intermediate node broadcasts the RREQ packets to its neighbor nodes if it is not the destination node. It updates its routing table and marks the entry for the reverse route. This process repeats until RREQ reaches destination or a node that has a valid route to destination.

On the destination side, when the destination node (node D) receives the RREQ packet, it replies with RREP packet that is unicasted along the reverse route of intermediate nodes (node D-A-S) until it reaches RREQ originating node. At the end of RREQ-RREP cycle, a bidirectional route is established between source and destination. Node S calls AODV's *recvReply*() function to update the routing table entry for node D if any one of the following conditions is satisfied.

i. The new destination sequence number provided in RREP packet is higher than the existing one in the routing table.

ii. If both the destination sequence numbers are equal, the hop count number is checked in RREP packet to confirm if it is smaller than existing one in the routing table.

Several studies have been made which investigate the performance of WSN and MANET under node misbehavior attacks. The effects of blackhole attack on AODV protocol is studied in [11]. A node under black hole attack declares itself the most suitable node to forward packets that have shortest path to the destination, but drops all the received packets. A blackhole node exploits the weakness of route discovery mechanism (RREP-RREQ packets) of reactive protocols, such as AODV, to drop all the packets in the network. The most critical influence of this attack on the network results in significantly dropping the packet delivery ratio.

In [12–14], studies have been made to investigate the performance of MANET in presence of wormhole attack. In wormhole attack, an adversary creates a connection (called *tunnel*) between two different points in the network that are not in communication range of each other. The two colluding nodes under wormhole attack capture packets at one end (source) and tunnel them to other end (destination) and replay them. To launch

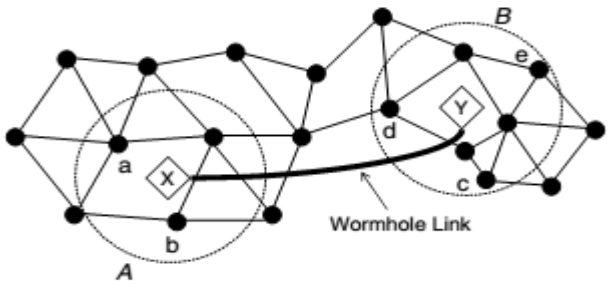

Fig. 2: A depiction of Wormhole attack [15]

wormhole attack, an adversary directly tunnels RREQ packet to the destination without increasing hop-count value. It disrupts proper routing mechanism of AODV and avoids other routes from being discovered. Once wormhole attack is established, malicious nodes may use it for launching other attacks such as packet drop attack and DoS attack. Figure 2 demonstrates a wormhole attack where two malicious nodes, X and Y, act as wormhole nodes.

X and Y replay every captured packet to each other through the tunnel linked between them. This attack propagates false information in the network and among the nodes in region A. The nodes in region A assume that the nodes in region B are their neighbors. As a result, the routing mechanism is badly affected. The authors in [12] employ *Packet Leash* and *Time of Flight* techniques to detect and prevent wormhole attack. In Packet leash, all nodes authenticate time and location information for every other node using symmetric key. In time of flight, a node estimates the round-trip time of a packet which helps in deciding whether the packets end up travelling further or return within round-trip time. The authors in [12] and [13] did not provide simulation based study to consider the effects of wormhole attack on AODV. The authors in [14] analyze the performance of AODV under wormhole attack only in terms of throughput with limited network parameters which is not sufficient to measure performance of MANET.

The authors in [7], [16], [17] investigate the performance of AODV protocol under grayhole attack. The performance is measured in terms of packet delivery ratio, packet drop ratio, throughput, normalized routing load and end-to-end delay. However, none of the work either analyzed the effect of grayhole attack in terms of consumed energy as it is most important design issue for WSN; neither provides countermeasures to defend attack.

The authors in [18] provide theoretical analysis of various node misbehavior attacks but none of the attacks is simulated on either proactive or reactive protocols to study the effects.

The authors in [19] conducted a simulation based study of SAODV for MANET to analyze the affect of grayhole attack. SAODV uses cryptographic extensions to provide authenticity and integrity of routing messages and all routing messages are digitally signed. However, the above proposal is security extensions of existing mobile ad-hoc routing protocols which is not suitable for resource constrained WSNs.

Most of the literature cited in this study relates to the MANET, but the network dynamics are different for WSN. To propose a secure routing protocol for WSN, impact of attacks must be analyzed under WSN. The secure routing protocol developed for mobile ad-hoc networks could not be directly used for wireless sensor network due to the following differences between two types of networks.

i. In most of the WSN applications, sensor nodes are static therefore topology changes are not as frequent as in mobile ad hoc networks where nodes are mobile. WSN topology may change due to some node failure or battery depletion. Therefore, secured routing protocol developed for MANET to cope with the node mobility and dynamic nature of network may contain features that are not required or are unnecessary for WSN.

ii. In WSN, the goal of sensor nodes is to send the sensed data to base station. Similarly base station could send control information to sensor nodes. Thus the communication type may be many-to-one and one-to-many. While in mobile ad hoc network, most of the communication is one-to-one. Therefore, secured routing protocol developed for one-to-one communication is not suitable for many-to-one and one-to-many communications.

iii. In MANET, the nodes are in the form of cell phones, PDAs or laptop class computes. These types of devices have much more resources (memory of hundreds or thousands of megabyte, large batteries and speedy processors) as compared to sensor nodes in WSN that are much more resource constrained. Therefore, secure ad-hoc network routing protocol that may use complex security mechanisms like public key cryptography cannot be directly used in sensor networks.

By keeping above mentioned points in mind, this work is conducted to analyze the impact of grayhole attack in WSN prior to propose a secure routing solution for WSN.

Furthermore, most of the discussed literature did not pay attention to measure the performance of a network in terms of consumed energy, neither provided counter-measures to defend grayhole attack. As WSN is a resource constraint network and energy is the most critical design parameter for providing secure solutions. Hence, it is necessary to study the impact of node misbehavior attacks on existing routing protocols to suggest a suitable secure routing protocol. In subsequent section, grayhole attack mechanism is discussed in detail.

3. GRAYHOLE ATTACK MECHANISM

In this paper, grayhole attack is considered as an attack model. In grayhole attack, a malicious node does not drop all the packets, but selectively drops the packets depending upon node-ID or packet type [20], [21]. The term "*selective*" means that the grayhole node may drop

packets of one type and forward packets of other types. For example, a grayhole node may drop packets from some set of nodes in the network, but forward packets from other set of nodes. Similarly, grayhole node may drop all TCP packets, but forward all UDP packets. In another form of grayhole attack, a grayhole node may drop packets for some time duration and act as misbehaving node, but switch to normal behavior at later time. Therefore, detection of grayhole nodes becomes very difficult.

Let us assume that a compromised node behaves like a grayhole node in the network and is denoted by *M*. The objective of node *M* is to drop packets for some time duration. The probability of dropping packets by node *M* is denoted by $P(M)$ and the probability of normal nodes (*N*) in the network is denoted by $P(N)$. The probability for the occurrence of grayhole attack in WSN is given by equation 1.

$$P(M) = \frac{P\left(\frac{M}{N}\right) * P(N)}{P(M)} \quad \ldots (1)$$

Algorithm-I depicts the algorithm for launching a grayhole attack. AODV code in NS2 has been modified to simulate grayhole attack in WSN. Initially, grayhole node behaves normally and sends genuine RREP message to the node that initiated RREQ message. Afterwards, grayhole node behaves maliciously and begins dropping packets.

Algorithm – I: Launching Grayhole Attack

```
if (Packet Type_AODV)
{
if(RREQ) {

if(I am the source or previously seen it) {
Drop the Packet
}

else if (No Attack)
{
Resolve the Route;
SendRouteReply;
else if (GrayHoleAttack) {
//Gray hole will send a genuine reply
Resolve the Route;
SendRouteReply;
}
}
}
else
{
Handle it in Normal way
}
}
else if  (it is a packet which I am originating) {
Handle it in Normal way
}
else {
//it is the packet I am forwarding
if (No Attack) {
Handle it in Normal way
}
}
else if(GrayHoleAttack) {
//Maliciously dropping the packet
Drop the Packet
}
```

4. SIMULATION MODEL

NS2 [22] is an event-driven simulator and has proved to be valuable in analyzing the dynamic nature of networks. NS2 has achieved remarkable reputation in network and communication research community due to its modular nature and flexible design. NS2 simulator has been extensively used to analyze the performance of AODV protocol in the presence of grayhole nodes.

Our evaluations are based on the simulation of variable number of sensor nodes (10, 20 and 30 nodes) as shown in Figure 3(a), 3(b) and 3(c) respectively. The nodes form a wireless senor network over a rectangular region (500×500 m). We also vary the number of grayhole nodes in the network to analyze the resulting effects.

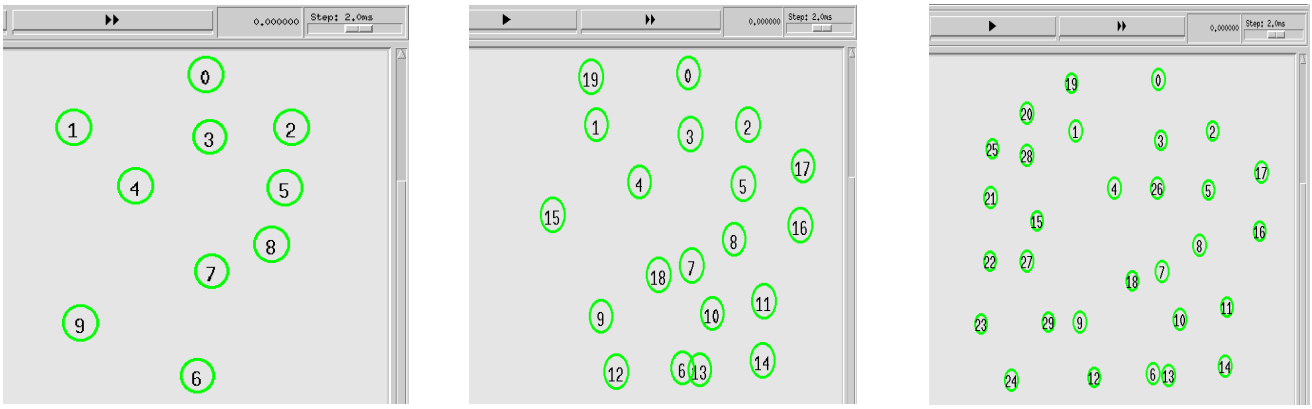

Fig. 3: (a) (b) (c)

Table 1 lists the parameter settings for our simulation environment.

TABLE 1: SIMULATION PARAMETERS

Simulation parameters	Values
Simulation Area	500 x 500 m
Routing protocol	AODV
Simulation Time	500 sec
Number of nodes	10, 20, 30
Number of grayhole nodes	0, 1, 2
Transport layer protocol	UDP
MAC	IEEE 802.15.4
Application layer traffic	CBR
Packet size	50 bytes

5. SIMULATION RESULTS

Performance of AODV protocol is measured in terms of packet delivery ratio, average end-to-end delay, number of packets dropped and average energy consumed. The performance is analyzed by using different simulation scenarios as mentioned below.

i. When there are 10 nodes in the network, with and without compromised nodes (grayhole nodes).

ii. When there are 20 nodes in the network, with and without compromised nodes (grayhole nodes).

iii. When there are 30 nodes in the network, with and without compromised nodes (grayhole nodes).

Figure 4 shows how the packet delivery ratio is affected in the presence of grayhole nodes. It is evident from the results that as the number of grayhole nodes increase in the network, packet delivery ratio decreases, leaving less number of packets to reach destination. Additionally, the grayhole nodes exhibit dual behavior. Sometimes, a grayhole node behaves like a normal node and obeys the routing rules. But at other time, it violates the rules of routing protocol by dropping packets in a random fashion. As a result, it does not drop all the received packets as contrast to blackhole attack where compromised nodes drop all the received packets. When there is no grayhole node in the network, PDR is almost 100% in all three scenarios. When grayhole nodes become part of the network, PDR drops to 32%, 21% and 10%, respectively, for three scenarios.

Figure 5 shows the result of average end-to-end delay for normal and compromised AODV. The simulation results depict that when there are no compromised nodes in the

network, it takes no time for the packet to reach destination. As the number of compromised nodes increase in the network, average end-to-end delay also increases as compromised nodes flood out false routing information in the network which prevent data packets to reach intended destination. If we compare the results of the three scenarios, we find that average end-to-end delay is significantly higher when there are more grayhole nodes in the network. It is almost increased by 80% in case of the third scenario.

Figure 6 shows how the packet drop ratio is affected with and without grayhole nodes. It is observed from the results that as the node density increases, packet drop ratio also increases. AODV in its normal form also drops some of the RREQ packets due to unavailability of a fresh route. The inherent feature of grayhole attack is to drop the packets randomly. One of the limitations with existing AODV is that it only generate single path while transferring packets to destination. If a grayhole node becomes the part of selected route, it drops packets randomly. Similarly, if number of grayhole nodes increases and becomes 1-hop neighbor of source node, it gets more leverage to be part of a chosen route. The number of packets dropped in the third scenario is significantly higher as compared to other two scenarios due to the aforementioned reason.

Figure 7 shows the result of average energy consumption for both AODV and compromised AODV. It is observed from the results that as the density of malicious nodes increases in the network, average energy consumption also increases due to adverse effects of grayhole attack on route discovery and route resolve mechanisms of AODV. Energy consumption is directly related to the number of transmitted and received messages either data or control. When a node comes under grayhole attack, it violates normal route discovery mechanism of AODV and generates increased number of RREQ and RREP packets which in results increase overall energy consumption of network.

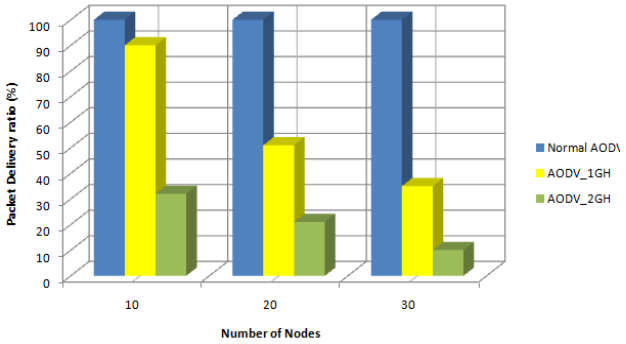

Fig. 4: Number of nodes vs. packet delivery ratio

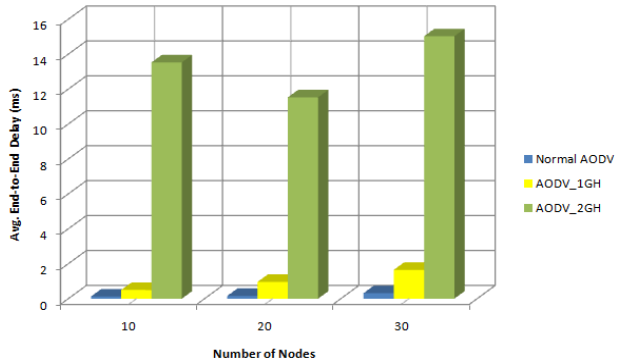

Fig. 5: Number of nodes vs avg. end-to-end delay

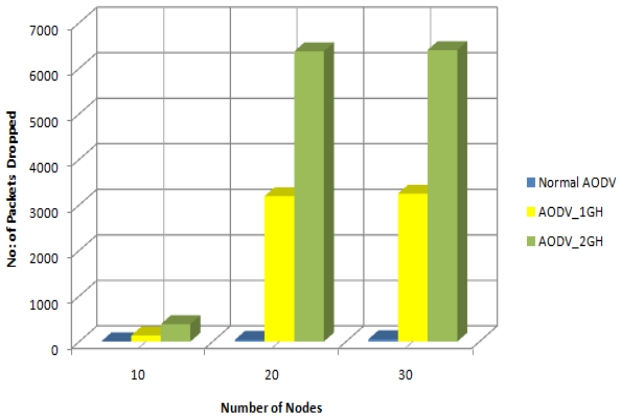

Fig. 6: Number of nodes vs. number of dropped packets

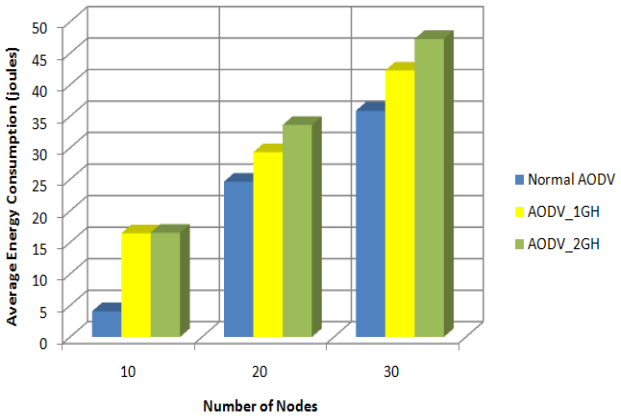

Fig. 7: Number of nodes vs. average energy consumption

6. COUNTERMEASURE AGAINST GRAYHOLE ATTACK

Routing in WSN is a cooperative process where routing information must be shared between all nodes on the route to destination. There might be a strong case that some malicious or misbehaving nodes (grayhole nodes) might exist on discovered route and may not fulfill the desired rules and regulations of the protocol. Nonetheless, some countermeasures are available as follows:

i. A number of attacks can be prevented if malicious nodes are prevented from participating in the routing process. Authentication methods can be used to determine whether the sensor node can participate in routing. SEAD [23] and Ariadne [24] are secure routing schemes based on authentication mechanism.

ii. The effect of grayhole attack may be minimized by employing multi-path routing approach [25], as packets may be routed through other available paths. However, this approach is feasible for only minimizing the impact of an attack but does not prevent attacks.

iii. Promiscuous mode [26] and IDS solutions [27] can be used to monitor the behavior of all neighboring nodes whether they behave normally or maliciously. If some malicious behavior is observed, IDS may trigger some action, for example, may alert neighboring nodes about the malicious activity.

iv. Trust and reputation based systems (TRMs) [28] may be used to detect and exclude malicious nodes. These systems facilitate the nodes to predict the behavior of other nodes and provide secure mutual interaction.

v. Game theory based approaches [29] are also useful in dealing with misbehaving nodes. These approaches assume that some greedy actions are performed by malicious nodes to gain better performance such as leveraging the operating point, "Nash Equilibrium" and higher share of bandwidth.

vi. The behavior of malicious nodes can also be identified by checking the sequence number of packets. If abnormal increase in the sequence number is identified, the particular node is considered as a misbehaving node.

vii. Some reward and punitive mechanisms may be incorporated in secure routing protocols so that the nodes complying with the protocol may be provided incentives, otherwise nodes may be punished.

7. CONCLUSION

In this paper, we analyzed the performance of AODV grayhole attacks. We compared AODV with compromised AODV in terms of packet delivery ratio, end-to-end delay, packet drop ratio and average energy consumption. Simulation results show how badly grayhole attack affects the performance of AODV. As the number of grayhole nodes increases in the network, the packet drop ratio and end-to-end delay also increases, while drastically decreasing the packet delivery ratio. This study would provide a great help for researcher conducting their research on route misbehavior attacks in sensor networks. During implementation of grayhole attack on AODV, some of the weaknesses of AODV protocols are highlighted. Simulation results also proved the same. Our future work in this direction will focus on implementing other node misbehavior attacks, such as blackhole attack and wormhole attack in WSN and providing efficient and trust-aware routing mechanism to counter such attacks. The major objective in the design of the proposed scheme is to conserve energy while routing packets that most of the existing trust-aware schemes lack.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] D. Bhattacharyya, T. Kim, and S. Pal, "A comparative study of wireless sensor networks and their routing protocols.," *Sensors*, vol. 10, no. 12, pp. 10506–23, Jan. 2010.

[3] P. Goyal, S. Batra, and A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks," *International Journal of Computer Applications*, vol. 9, no. 12, pp. 11–15, 2010.

[4] V. S. Abel, "Survey of Attacks on Mobile Adhoc Wireless Networks," *International Journal on Computer Science and Engineering*, vol. 3, no. 2, pp. 826–829, 2011.

[5] C. Gupta, K. Gupta, and V. Gupta, "Security Threats in Sensor Network and their Possible Solutions," *International Symposium on Instrumentation & Measurement, Sensor Network and Automation (IMSNA)*, pp. 11–13, 2012.

[6] A. Ahmed, K. A. Bakar, and M. I. Channa, "Performance Analysis of Adhoc on Demand Distance Vector Protocol," *Journal of Computer Science*, vol. 10, no. 9, pp. 1466–1472, 2014.

[7] K. Pavani and D. Avula, "Performance of Mobile Adhoc Networks in Presence of Attacks," *International Conference on Information Security and Artificial Intelligence (ISAI)*, no. Isai, pp. 147–153, 2012.

[8] A. Jain, K. Kant, and M. . Tripathy, "Security Solutions for Wireless Sensor Networks," *Advanced Computing & Communication Technologies (ACCT), Second International Conference on*, pp. 430–433, 2012.

[9] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Computing and Information Sciences*, vol. 1, no. 1, pp. 1–16, 2011.

[10] C. E. Perkins, E. Belding-Royer, and S. Das, "RFC 3561-Ad hoc On-demand Distance Vector (AODV) routing," *Internet RFCs*, pp. 1–38, 2003.

[11] M. Roopak and B. Reddy, "Blackhole Attack Implementation in AODV Routing Protocol," *International Journal of Scientific & Engineering Research*, vol. 4, no. 5, pp. 402–406, 2013.

[12] A. A. Bhosle, T. P. Thosar, and S. Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET," *International Journal of Computer Science, Engineering and Applications (IJCSEA)*, vol. 2, no. 1, pp. 45–54, 2012.

[13] R. H. Jhaveri, A. D. Patel, J. D. Parmar, and Bh. I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 10, no. 4, pp. 12–18, 2010.

[14] A. Ratmele and R. Dhakad, "Performance Analysis of AODV under Worm Hole Attack through Use of NS2 Simulator," *International Journal of Engineering Research and Applications (IJERA)*, vol. 3, no. 3, pp. 201–205, 2013.

[15] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," *26th IEEE International Conference on Computer Communications.*, pp. 107–115, 2007.

[16] G. Usha and S. Bose, "Impact of Gray Hole Attack on Adhoc networks," *International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 404–409, 2013.

[17] Usha and Bose, "Comparing the Impact of Black Hole and Gray Hole Attacks in Mobile Adhoc Networks," *Journal of Computer Science*, vol. 8, no. 11, pp. 1788–1802, Nov. 2012.

[18] K. Xing, S. S. R. Srinivasan, M. Rivera, J. Li, and X. Cheng, "Attacks and Countermeasures in Sensor Networks : A Survey," *Network Security*, pp. 251–272, 2010.

[19] O. V Chandure, A. P. Bakshi, S. P. Tidke, and P. M. Lokhande, "Simulation of Secure AODV in Gray Hole Attack," *International Journal of Advances in Engineering & Technology (IJAET)*, vol. 5, no. 1, pp. 67–76, 2012.

[20] A. P. Renold, R. Poongothai, and R. Parthasarathy, "Performance analysis of LEACH with gray hole attack in Wireless Sensor Networks," *International Conference on Computer Communication and Informatics*, pp. 1–4, 2012.

[21] W. Zada Khan, Y. Xiang, M. Y Aalsalem, and Q. Arshad, "The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures," *International Journal of Wireless and Microwave Technologies (IJWMT)*, vol. 2, no. 2, pp. 33–44, Apr. 2012.

[22] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*, 2nd ed. Springer, 2012.

[23] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175–192, Jul. 2003.

[24] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Wireless Networks*, vol. 11, no. 1–2, pp. 21–38, Jan. 2005.

[25] E. Stavrou and A. Pitsillides, "A survey on secure multipath routing protocols in WSNs," *Computer Networks*, vol. 54, no. 13, pp. 2215–2238, Sep. 2010.

[26] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *6th Annual International Conference on Mobile Computing and Networking*, pp. 255–265, 2000.

[27] M. A. Rassam, M. A. Maarof, and A. Zainal, "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks," *American Journal of Applied Sciences*, vol. 9, no. 10, pp. 1636–1652, Oct. 2012.

[28] R. Roman, M. C. Fernandez-Gago, and J. Lopez, "Trust and Reputation Systems for Wireless Sensor Networks," *Security and Privacy in Mobile and Wireless Networking*, pp. 105–128, 2009.

[29] D. M. Shila and T. Anjali, "A Game Theoretic Approach to Gray hole attacks in Wireless Mesh Networks," *Military Communications Conference (MILCOM)*, pp. 1–7, 2008.