ANALYSIS OF AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL AGAINST NODE MISBEHAVIOR ATTACKS IN WIRELESS SENSOR NETWORKS

Adnan Ahmed*, Umair Ali Khan*, Adnan Rajpar**

ABSTRACT

Wireless Sensor Networks (WSN) have gained remarkable appreciations over the last few years. Despite significant advantages and tremendous applications, WSN is vulnerable to variety of attacks. Due to unattended nature of WSN, sensor nodes are more prone to be overtaken by an adversary. By doing that, an adversary can learn the contents of the victim's memory, can have access to valid cryptographic keys, and can also modify the behavior of corrupted nodes. In this paper, we investigate some of the most severe node misbehavior attacks in WSN, namely blackhole and grayhole attacks, using Ad-hoc On Demand Distance Vector (AODV) routing protocol. A detailed NS2 based implementation and comparative analysis of these attacks has been presented. The performance of AODV is evaluated by considering different metrics such as packet delivery ratio, packet drop ratio, average end-to-end delay, normalized routing load, and energy consumption. Simulation results are provided to show the effects of these attacks on AODV protocol which suffers from increased packet loss and decreased delivery ratio. Some counter measures against node misbehavior attacks are also provided.

Keywords*: AODV; grayhole attack; wireless sensor networks; security; node misbehavior; blackhole attack.*

1. INTRODUCTION

Wireless Sensor Network is a self-organized network comprising of individual nodes that connect with their surroundings by sensing or controlling physical parameter. A wireless sensor node is equipped with micro-sensor technology that has low computational power, low signal processing power, limited energy resources and short-rage communication facility [1]. Recent advances in computing and communication have enabled wireless sensor network to be deployed in variety of applications such as battle field monitoring, battle damage assessment, environmental monitoring, smart environments, monitoring the status of structures such as bridges, factory process control and automation, vehicle tracking and detection and monitoring disaster area [2].

Sensor nodes are placed in large number in hostile environments, which makes it difficult to protect them against tampering or captured by an adversary force that can launch attacks to make a node compromised and can have easy access to valid keys and memory contents [3]. This unattended nature of WSN makes sensor nodes vulnerable to node physical capture, selfish and malicious behavior of nodes. Routing in WSN is a cooperative process where routing information must be shared between all the nodes on the route to destination. There might be a strong case that some malicious, selfish or misbehaving nodes might exist on a discovered route and may not fulfill the desired rules and regulations of the protocol. In this study, we will analyze the impact of two types of node misbehavior attacks: blackhole and grayhole.

Prior to proposing a secure solution to protect WSN against the aforementioned node misbehavior attacks; it is important to gain full understanding of how these attacks are launched. The major objective of this paper is to analyze how these attacking nodes exploit the weakness of a route discovery mechanism of a routing protocol and work maliciously. Most of the existing studies on performance evaluation of WSN mainly focus on investigating the impact of attacks without providing solutions to avoid them. WSN is a resource constraint network and energy is most critical design parameter for providing secure solutions, but most of the literature did not pay much attention to analyze the impact of attacks on the overall energy consumption of the network. In this study, along with providing countermeasures against node misbehavior attacks, impact of the attacks is also investigated and analyzed with justified parameters for WSN.

The rest of the paper is organized as follows. Section 2 provides the overview of blackhole attack and grayhole attack; and also discusses the related work in this domain. Section 3 presents the simulation model for simulating attacks. Section 4 presents the simulation results with analysis. Section 5 provides some countermeasures against node misbehavior attacks. Section 6 concludes the paper with some potential future work.

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

2. BLACKHOLE AND GRAYHOLE ATTACK MECHANISM

In this paper, blackhole and grayhole attacks are considered as an attack model. In a blackhole attack [4–6], a compromised node claims itself to be the most suitable forwarding node but refuses to cooperate with routing rules and drops all the received packets. A malicious node advertises itself to have fresh and optimal path to the destination by exploiting weaknesses of the route discovery packets (RREQ and RREP). A blackhole node sends false RREP packets to attract most of the network traffic by incorporating highest sequence number in RREP packets. Figure 1 shows the behavior of blackhole node in a network using AODV routing protocol.

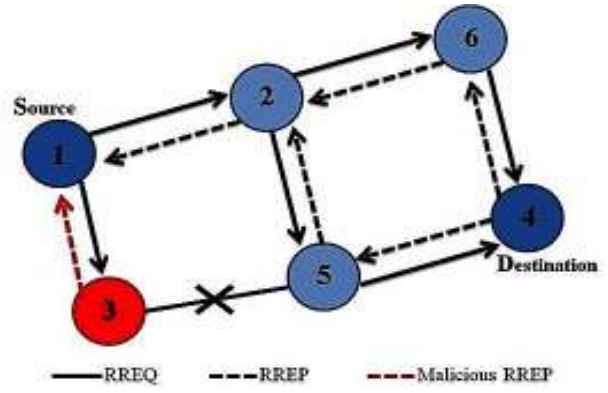

Figure 1: Blackhole attack

As shown in Figure 1, when a source node wants to send packets to destination node, it broadcasts RREQ packets. The node receiving RREQ packets responds with RREP packets. The malicious node (node3) sends a false RREP packet with highest sequence number indicating it has better route to destination. The source node assumes that the provided information is true. Therefore, it sends packets to the malicious node. The malicious node exhibiting blackhole behavior drops all the received packets, leaving none or very few packets to reach the destination. The most critical influence of this attack on the network results in severely diminishing the packet delivery ratio.

A compromised node against grayhole attack drops packets selectively rather than dropping all received packets [7–9]. The selective dropping depends on the type of packets or group of some nodes. For example, a grayhole attacker node forwards UDP packets while dropping TCP packets. Another malicious behavior of the very attack is to drop packets for particular time duration and at later time switching its behavior to normal node. The grayhole node sends genuine route-reply packets in contrast to blackhole nodes where they send fake route-reply to attract most of network traffic. Due to the aforementioned behaviors of grayhole node, detection becomes very difficult [10][11].

Let us assume that the grayhole node is represented by M, with aim to drop packets for some time period. Let $P(M)$ denotes the probability for dropping packets for grayhole node and $P(N)$ denotes the probability of normal nodes. The probability for the occurrence of grayhole attack in WSN is given by equation 1.

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

3. RELATED WORK

The relevant literature shows a number of studies investigating the performance of WSN and MANET under node misbehavior attacks. The authors in [12–14] provide theoretical analysis of various node misbehavior attacks, but none of the attacks is simulated on either of proactive or reactive protocols to study the effects of the attacks.

In [15–17], the performance of MANET in presence of wormhole attack is analyzed. In wormhole attack, an adversary creates a connection (called tunnel) between two different points in the network that are not in the 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. The authors in [15] implement Packet Leash and Time of Flight techniques to detect and prevent a wormhole attack. The authors in [15][16] do not provide any simulation based study to consider the effects of wormhole attack on AODV. The authors in [17] analyze the performance of AODV under a wormhole attack only in terms of throughput with limited network parameters which is not sufficient to measure performance of a MANET.

The authors in [10] analyze the performance of LEACH protocol against a grayhole attack. LEACH protocol is designed for resource constrained WSN where energy consumption is a critical factor. However, the impact of the attack on overall energy consumption of nodes is not given consideration in this study. The relevant literature provides various other studies where impact of attacks on routing protocol has been investigated [16][18–22]. Most of the studies mainly target generic ad-hoc networks which provide powerful hardware platform with enough storage, energy, memory and processing resources but the dynamics of WSN are different where sensor nodes with limited resources are deployed in the network. Furthermore, most of the studies do not pay attention on analyzing the performance in terms of energy consumption and do not provide appropriate measures to

defend those attacks. In order to propose an optimal solution for WSN, the impact of attacks must be analyzed under resource-constrained environment of WSN.

4. THE SIMULATION MODEL

Network Simulator-2 (NS-2), an event based simulator, has achieved tremendous appreciations in network and communication research community due to its capability of analyzing the dynamic nature of networks, its flexible design and modular nature [23]. In this study, performance of AODV and Compromised-AODV (C-AODV) protocols has been analyzed under blackhole and grayhole attacks. The performance of AODV routing protocol is evaluated under these attacks by considering different performance parameters such as packet delivery ratio, packet drop ratio, end-to-end delay, normalized routing load and overall energy consumption of sensor nodes.

Our evaluations are based on the simulation of variable number of malicious nodes (blackhole and grayhole nodes). Fifty sensor nodes are randomly placed to form a wireless senor network over an area of 1000m × 500 m. There are 4 source nodes placed at different locations which transmit packets at specified time period, and one sink node that is placed in the center of network topology. Table 1 lists the parameter settings for our simulation environment.

Table 1: The simulation parameters

Simulation parameters	Values
Simulation Area	1000 x 500 m^2
Simulation Time	1000 sec
Routing protocol	AODV, C-AODV
Number of sensor nodes	50
Number of Malicious nodes	0, 1, 2, 3, 4
Transport layer protocol	UDP
Initial Node Energy	50 joules
Packet size	50 bytes
Node Mobility	Random
MAC protocol	IEEE 802.15.4
Application layer traffic	CBR

5. EXPERIMENTAL RESULTS AND DISCUSSION

In this study, we analyze how AODV behaves under various number of blackhole and grayhole nodes. Figure 2 shows that when neither of the attack is launched on AODV, Packet Delivery Ratio (PDR) is 97%. When the number of malicious nodes increases in the network, PDR deteriorates. For a blackhole attack, it drops to 70%, 58%, 24% and 2% when there are 1, 2, 3 and 4 blackhole nodes in the network, respectively. For grayhole attack, PDR drops to 74%, 60%, 55% and 42% when there are 1, 2, 3, and 4 grayhole nodes in the network, respectively. Both attacks bring delivery ratio to unacceptable ranges but blackhole attack proves to be more packet-hungry. A compromised node under a blackhole attack sends fake RREP packets informing other nodes that it has the shortest route to destination while dropping all the received packets, leaving none or few packets to reach destination. A grayhole node, on the other hand, sends genuine RREP packets but switches its behavior from normal to malicious or vice versa.

Figure 3 shows average end-to-end delay comparison for AODV and C-AODV. Under normal scenario, packets reach destination within minimum delay. As the density of misbehaving nodes increases, average end-to-end delay also increases. The average end-to-end delay increases by 45% and 80% for grayhole and blackhole attacks respectively, in case where 4 misbehaving nodes are part of the network. Such increased delay caused by both grayhole and blackhole attacks are not acceptable for mission critical applications.

Figure 4 shows the number of dropped packets in the network having some malicious nodes. It is observed that as the density of malicious nodes increases, the number of packet drop also increases, as it is inversely proportional to delivery ratio. Due to the inherent characteristic of high packet drop by blackhole node, the number of dropped packets by a blackhole node is higher than a grayhole node for all cases that probabilistically drop packets leaving a few or more packets reaching the destination.

Figure 5 shows how the normalized routing overload is affected in the presence of misbehaving nodes. As number of misbehaving nodes increases in the network, Normalized Routing Load (NRL) also increases. NRL refers to the ratio of total number of transmitted control packets to the total number of received data packets.

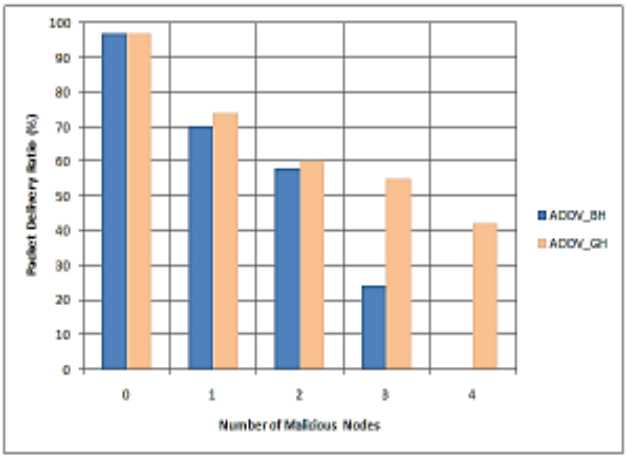

Figure 2: Number of malicious nodes vs. packet delivery ratio

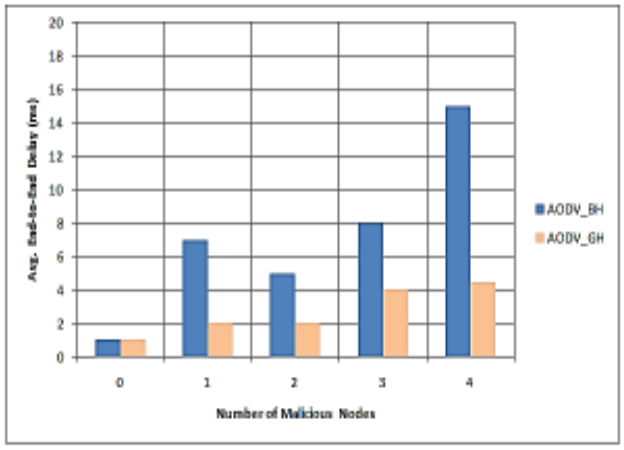

Fig. 3: Number of malicious nodes vs. avg. End-to-end delay

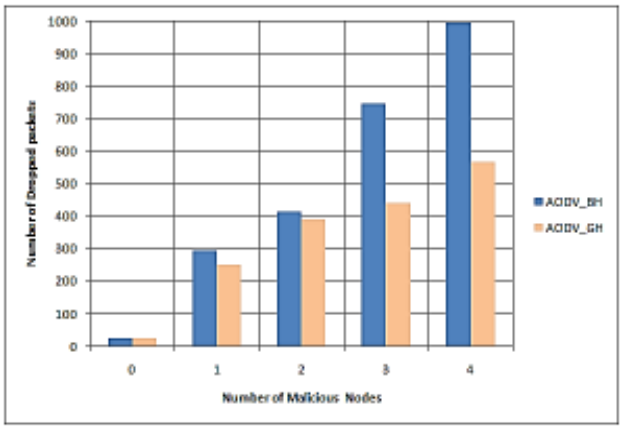

Fig. 4: Number of malicious nodes vs. number of dropped packets

A blackhole node sends false RREP packets and generates additional routing packets which leads to high routing load as compared to a grayhole node. As WSN is a resource-constrained network, such increased overload may badly affect the lifetime of the network.

Figure 6 shows comparison of average energy consumption for both AODV and C-AODV. The energy consumption is directly related to the number of transmitted and received messages (data or control). Simulation results show that as the number of misbehaving nodes increases, average energy consumption also increases due to the adverse effects of the misbehaving nodes on route discovery and route resolve mechanisms of AODV. The increased number of route maintenance calls and route discovery control packets increases overall energy consumption of the network, when it comes under a number of compromised nodes. Such increased energy consumption is not feasible for battery powered sensor nodes which mostly operate in unattended environments.

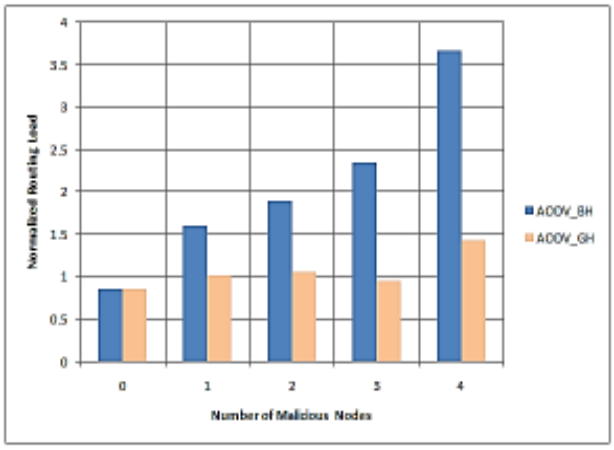

Fig. 5: Number of malicious nodes vs. normalized routing load

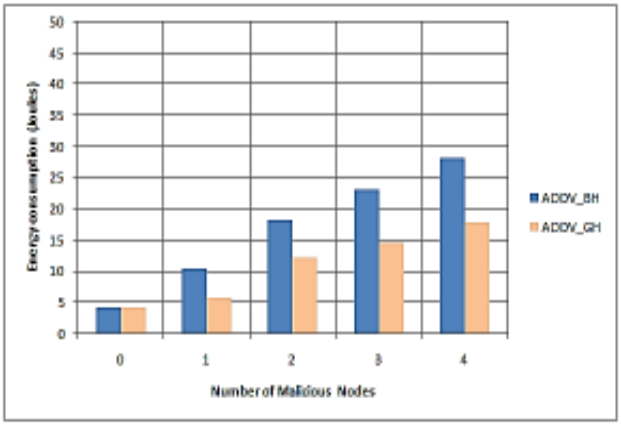

Fig. 6: Number of malicious nodes vs. energy consumption

6. COUNTERMEASURES AGAINST NODE MISBEHAVING ATTACKS

Multi-hop communication requires the exchange of routing information among intermediate nodes. However, multi-hop communication also raises the problem to securely route packets as some misbehaving nodes may become part of the active route to destination. Nonetheless, following defense mechanisms can be adopted for a secure routing.

i. Verifying packet sequence number can be helpful, in few cases, for the detection of misbehaving nodes. A node is considered as a misbehaving node if an abnormal increase in the sequence number is identified.

ii. Secure routing protocols may exploit some mechanisms for providing rewards and punishments based on the behavior of nodes. If a node cooperates in packet forwarding, it may be provided rewards, otherwise punished.

iii. Authentication methods can be used to determine whether the sensor node can participate in routing or

not. SEAD [24] and Ariadne [25] are the two secure routing protocols based on an authentication mechanism which prevent misbehaving nodes to become part of the network.

iv. Game theory based approaches [26] are also useful in dealing with misbehavior 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.

v. Intrusion detection [27][28] and watchdog [29][30] solutions may be used for monitoring the behavior of nodes. If some malicious behavior is observed, an appropriate action may be triggered like alerting neighboring nodes.

vi. Trust and Reputation based systems [31][32] may be used for detection and isolation of malicious nodes. These systems facilitate the nodes to predict the behavior of other nodes and provide secure mutual interaction.

vii. Exploiting the multi-path routing approach [33] may minimize the adverse effects of misbehaving nodes due to the availability of backup paths. However, this approach is only responsible for minimizing the impact, but does not completely prevent the attack.

7. CONCLUSION

In this study, we comprehensively analyzed the performance of WSN against the most severe node misbehaving attacks such as blackhole and grayhole attacks. NS2 simulator has been used to simulate these attacks using AODV routing protocol. The performance is evaluated in terms of packet delivery ratio, number of dropped packets, average end-to-end delay, average throughput, normalized routing load and energy consumption. Simulation results show how badly these attacks affect the overall performance of a WSN. As the number of misbehaving nodes increases in the network, it badly affect the overall performance of the network and brings the delivery ratio to an unacceptable range. Some countermeasures against node misbehavior attacks are also provided. This analysis is helpful to gain insight into the unexpected anomalies in a WSN and envisaging appropriate counter-measures. Our future work in this direction will focus on implementing other node misbehavior attacks, such as sinkhole attack, Sybil attack, HELLO flood attack, selfishness and wormhole attack in WSN and providing efficient and trust-aware routing mechanisms to counter such attacks.

REFERENCES

[1] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Ad Hoc Networks, vol. 3, no. 3, pp. 325–349, May 2005.

[2] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," Computer Networks, vol. 51, no. 4, pp. 921–960, Mar. 2007.

[3] M. Momani and S. Challa, "Survey of Trust Models in Different Network Domains," International Journal of Ad hoc, Sensor & Ubiquitous Computing, vol. 1, no. 3, pp. 1–19, 2010.

[4] 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.

[5] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing security in ad hoc wireless networks," in Network Security, S. C.-H. Huang, D. MacCallum, and D.-Z. Du, Eds. Boston, MA: Springer US, 2010, pp. 117–142.

[6] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile Ad Hoc networks," in Proceedings of the 42nd annual Southeast regional conference on - ACM-SE 42, 2004, p. 96.

[7] S. Chundong, P. Yi, J. Wang, and H. Yang, "Intrusion Detection for Black Hole and Gray Hole in MANETs," KSII Transactions on Internet and Information Systems, vol. 7, no. 7, pp. 1721–1736, 2013.

[8] M. Arya and Y. K. Jain, "Grayhole Attack and Prevention in Mobile Adhoc Network," International Journal of Computer Applications, vol. 27, no. 10, pp. 21–26, 2011.

[9] S. Ramachandran and V. Shanmugam, "Performance Comparison Of Routing Attacks In Manet And Wsn," International Journal of Ad hoc, Sensor & Ubiquitous Computing, vol. 3, no. 4, pp. 41–52, 2012.

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

[11] 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.

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

[13] S. Mohammadi, R. E. Atani, and H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks," Journal of Information Security, vol. 02, no. 02, pp. 69–84, 2011.

[14] J. young Kim, R. D. Caytiles, and K. J. Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks," Journal of Security Engineering, vol. 9, no. 3, pp. 241–250, 2012.

[15] 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.

[16] 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.

[17] 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.

[18] I. Hababeh, I. Khalil, A. Khreishah, and S. Bataineh, "Performance Evaluation of Wormhole Security Approaches for Ad-hoc Networks," Journal of Computer Science, vol. 9, no. 12, pp. 1626–1637, 2013.

[19] H. Simaremare and R. F. Sari, "Performance Evaluation of AODV variants on DDOS , Blackhole and Malicious Attacks," International Journal of Computer Science and Netowrk Security (IJCSNS), vol. 11, no. 6, pp. 277–287, 2011.

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

[21] V. Bibhu, K. Roshan, K. B. Singh, and D. K. Singh, "Performance Analysis of Black Hole Attack in Vanet," International Journal of Computer Network and Information Security, vol. 4, no. 11, pp. 47–54, Oct. 2012.

[22] S. Sharma and R. Gupta, "Simulation Study Of Blackhole Attack In The Mobile Ad Hoc Networks," Journal of Engineering Science and Technology, vol. 4, no. 2, pp. 243–250, 2009.

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

[24] 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.

[25] 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.

[26] Y. B. Reddy and S. Srivathsan, "Game theory model for selective forward attacks in wireless sensor networks," in Control and Automation, 2009. MED'09. 17th Mediterranean Conference on, 2009, pp. 458–463.

[27] M. Tiwari, K. V. Arya, R. Choudhari, and K. S. Choudhary, "Designing Intrusion Detection to Detect Black Hole and Selective Forwarding Attack in WSN Based on Local Information," in Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on, 2009, pp. 824–828.

[28] T. Sharma, M. Tiwari, P. kumar Sharma, M. Swaroop, and P. Sharma, "An Improved Watchdog Intrusion Detection Systems In Manet," International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 3, pp. 1–4, 2013.

[29] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, pp. 255–265.

[30] E. Hernandez-Orallo, M. D. Serrat, J. Cano, C. T. Calafate, and P. Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," Communications Letters, IEEE, vol. 16, no. 5, pp. 642–645, 2012.

[31] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, "Trust management in wireless sensor networks," European Transactions on Telecommunications, vol. 21, no. 4, pp. 386–395, 2010.

[32] O. Khalid, S. U. Khan, S. A. Madani, K. Hayat, M. I. Khan, N. Min-Allah, J. Kolodziej, L. Wang, S. Zeadally, and D. Chen, "Comparative study of trust and reputation systems for wireless sensor networks," Security and Communication Networks, vol. 6, no. 6, pp. 669–688, 2013.

[33] M. Chakraborty and N. Chaki, "ETSeM: A Energy-Aware, Trust-Based, Selective Multi-path Routing Protocol," in Computer Information Systems and Industrial Management, 2012, pp. 351–360.