The Efficient Prevention of Wormhole Attack in AODV Routing Protocol in Wireless Sensor Networks

Bhavneet Kaur, Dr. Sandeep Singh Kang

Abstract— Wireless sensors networks (WSNs) consist of a large number of tiny, spatially distributed, and autonomous devices, called sensor nodes. The latter are equipped with sensing, computation, and wireless communications capabilities, and have very limited resources. Wireless sensor networks have been widely used in remote areas, military scenarios, sensing motion applications, agriculture solutions and natural disaster hitted areas. Interest in the area of Wireless sensor networks is growing since last few years because of its practical applications. These networks are equipped with large number of sensors, which are spatially distributed. Wireless sensor networks are widely used in remote areas, defense and military scenarios. Hence, their security is critical issue. They are more vulnerable to attacks than wired networks. Wireless sensor networks suffer from various active and passive attacks. One of such type of attack is Wormhole attack. In this, pair of nodes creates a virtual tunnel in the network. The malicious node at one end, capture the packets and tunnel them to another malicious node. Wormhole is a severe attack which can affect the route discovery process of the network. In this paper, we propose a solution to the wormhole attack in one of the most prominent AODV (ad-hoc on demand distance vector) routing protocol. The proposed method works for the detection and prevention of the wormhole attack in sensor networks. In the proposed method, a sensor can detect the fake neighbors which are caused by wormhole through the neighbor discovery process, and then a Manhattan Distance algorithm is used to detect and prevent wormhole attack according to the neighbor information and the broadcasting nature for distinct and reliable communication. Manhattan algorithm makes the broadcasting and packet forwarding more reliable and secure and furthermore prevents the simulation from any malicious attack. The proposed method reduces the delay in the network to a considerable extent thereby enhancing the performance.

Index Terms— Wormhole attack, Wireless sensor networks, sensor nodes, Isolator, Manhattan Distance formula , AODV, Malicious Node

1. INTRODUCTION

Wireless sensor networks are composed of a large number of sensor nodes. These nodes communicate with each other via wireless transmission [2]. Wireless sensor networks(WSNs) are playing a promising role in a variety of application areas, such as military, home applications and environment monitoring. For example, in emergency response operations such as after a natural disaster like a flood, tornado, hurricane, or earthquake, sensor networks could be used for real-time safety feedback, regular communication networks may be damaged, so emergency rescue teams might rely upon sensor networks for communication. Many sensor networks have mission-critical tasks, such as above military applications, thus it is clear that security needs to be taken into account at the time of design.

Wireless Sensor Networks have several unique characteristics that make them distinguishable from traditional wireless networks. First of all, WSNs generally operate in unattended areas and contain a large number of sensor nodes, which can be in the order of thousands. These nodes have strictly limited resources in terms of energy, memory, communication and computation. Due to such resource constraints, reliability and precision of a single sensor node is significantly low thereby requiring collaborative data collecting and processing. In addition, because of the simple and unreliable hardware, sensor nodes may die earlier than their expected lifetime. Hence, the number of sensor nodes may be changed in the network lifetime in a dynamic topology.
The open nature of the wireless communication channel, the lack of infrastructure, the fast deployment practices and the

- *Bhavneet Kaur is currently pursuing masters degree program in computer science engineering from CEC, Landran, PTU, India, E-mail: neet_punjabi@yahoo.co.in*
- *Dr. Sandeep Singh Kang is working at CGC, Landran as HOD (CSE) , India, E-mail: sskang4u1@rediffmail.com*

hostile deployed environments, make these networks vulnerable to various security attacks [3]. These attacks are generally classified as active and passive attacks [6]. A passive attack does not affect the normal functionality of a network. A passive attack can be capturing data without altering it. The active attacks are categorized as external and internal attacks. An attack from within the network is an internal attack whereas an attack from a foreign network is an external attack. In most wireless networks, an attacker can easily inject bogus(fake) packets, impersonating another sender [1]. We refer to this attack as a spoofing attack. An attacker can also easily eavesdrop on communication, record packets, and replay the (potentially altered) packets.

One of the severe attacks in Wireless sensors network is Wormhole attack. In this, two attackers are connected via high speed link called the wormhole link or tunnel [4]. Once the link is established, the malicious node can record the data they overhear, forward it to other colluding node and can replay the packets. The tunneling procedure generates an illusion that the two nodes more than one hop away are in the neighborhood of each other [7].

In this paper, we will detect and defend against a severe attack in wireless, which we call a wormhole attack, and we present a new, general mechanism for detecting and thus defending against wormhole attack in AODV routing protocol. This paper is organized as follows: Section II discusses the AODV routing protocol and wormhole attack, Section III presents the Proposed Scheme, Section IV contains results and discussions. Finally we conclude in Section VI.

2. AODV ROUTING PROTOCOL AND WORMHOLE ATTACK

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. . It is an on-demand and distance-vector routing protocol, means that a route is established by AODV from a destination only on demand i.e. whenever needed. AODV is capable of both unicast and multicast routing. It keeps these routes as long as they are required by the sources. The sequence numbers are used by AODV to ensure the freshness of routes.

AODV defines three types of control messages for route maintenance: RREQ- A route request message is transmitted by a node requiring a route to a node [6]. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ). Every node maintains two separate counters: a node sequence number and a broadcast-id. The RREQ contains the following fields. The pair <source address, broadcast ID> uniquely identifies a RREQ. Broadcast id is incremented whenever the source issues a new RREQ. RREP- A route reply message is unicast back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator. RERR- Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a “precursor list'', containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

Route discovery process in AODV is vulnerable to wormhole attack. When an RREQ message is generated by source, the intermediate nodes that have fresh path to the destination node may respond to the RREQ message. If a malicious node listens to the RREQ message, it responds to the request claiming that it has the shortest and the freshest path to the destination. As a result, the route via malicious node is selected which easily misroute the network traffic to it and can further drop the packets.

To provide a general description of the attack, we consider the example of Figure 1. Sensor node A sends a message to the Base station (BS). Typically, two routes can be established: $C \rightarrow D \rightarrow H \rightarrow I \rightarrow K \rightarrow F$ or $B \rightarrow D \rightarrow E$. Node C is malicious and colludes with node F to attract the traffic through it. To do so, it tunnels the received messages using a low latency link to the opposite end of the wormhole. In the case of reactive routing protocols, when node A wants to establish a route to the destination, node C sends a route request packet through the tunnel making it arrive sooner or with shorter hop count [5]. Consequently, the BS and the node A are mislead and be forced to choose the first route, which appears to be equal to $C \rightarrow F$ and shorter than the second route. The tunnel can be established by the use of packet encapsulation, high powered transmission, and out-of bound channel establishment.

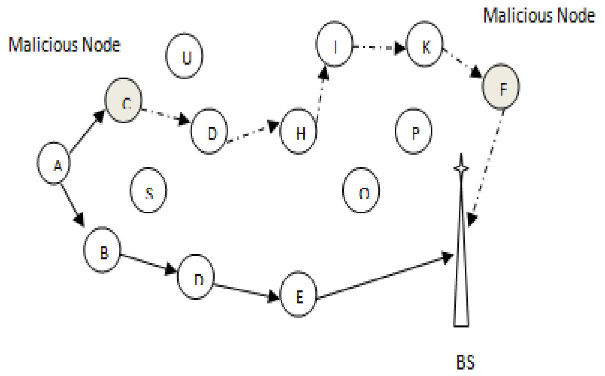


Figure 1: Wormhole attack in WSNs

3. PROPOSED SCHEME FOR WARMHOLE DETECTION AND PREVENTION

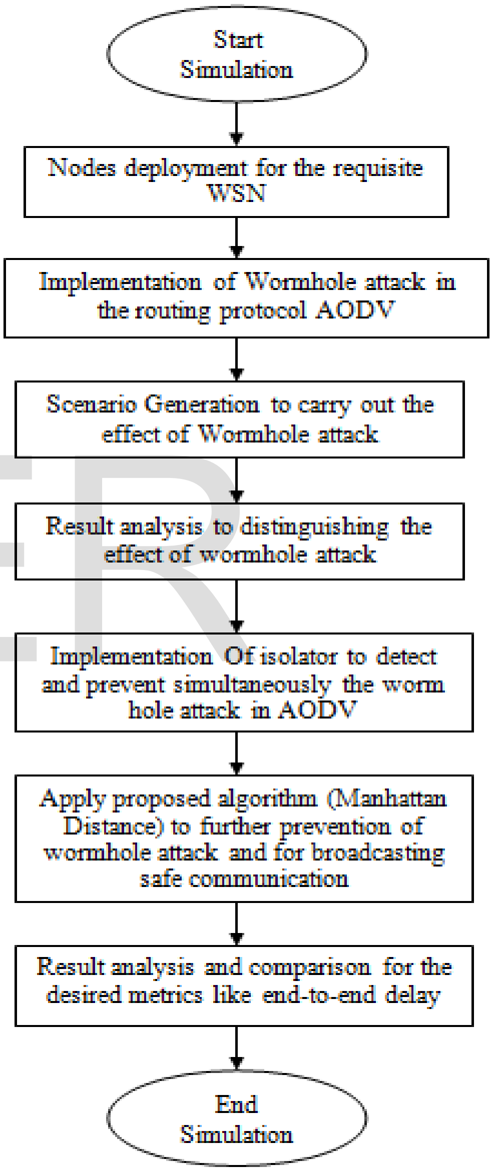
The objective of the work is to improve the routing protocol by detecting and defending against the malicious Wormhole nodes thereby by increasing the security and improving the performance of the network and AODV routing protocol. In order to achieve this goal, the misbehaving or malicious nodes are to be identified and then proper mechanism is applied to defend against that malicious node in the network. The proposed work is about detection and prevention of wormhole attack between the communication taken place between the source and the destination. The technique works on both hidden and exposed wormhole attack. The term "isolator" is used for the mechanism that will detect the existence of wormhole and will try to limit its affect in the network. Further, Manhattan distance algorithm will work for long term detection and prevention of the wormhole attack.

Algorithm:

Step 1: Route request send to all intermediate nodes between source S and destination D.

Step 2: Route discovery for shortest and freshest path using AODV.
Step 3: Generation of Neighbor list.
Step 4: Detection of wormhole nodes using isolator and minimize its effect.
Step 5: Use Manhattan distance formula for further detection and prevention. It states that the distance between two points is measured along axes at right angles. In a plane with p1 at $(x_1\ , y_1)$ and p2 at (x_2, y_2), it is $|x_1 - x_2| + |y_1 - y_2|$.
Step 6: Result comparison between wormhole hitted scenario and proposed scheme for defending against wormhole.

Flowchart Diagram:


Start Simulation
Nodes deployment for the requisite WSN
Implementation of Wormhole attack in the routing protocol AODV
Scenario Generation to carry out the effect of Wormhole attack
Result analysis to distinguishing the effect of wormhole attack
Implementation Of isolator to detect and prevent simultaneously the worm hole attack in AODV
Apply proposed algorithm (Manhattan Distance) to further prevention of wormhole attack and for broadcasting safe communication
Result analysis and comparison for the desired metrics like end-to-end delay
End Simulation

4. RESULTS AND DISCUSSION

The proposed system is implemented in NS2 environment. AODV routing protocol is used to implement the algorithm. Here the basic parameters of the proposed work are presented respective to the simulation environment in table 1.

Table 1: Simulator Parameters

Parameter	**Value**
Simulator	NS-2
Simulator duration	90 sec
Topology	2500 meter X 2500 meter
No. of nodes	100
Maximum segment size	512 bytes
Traffic type	FTP (tcp)
Routing Protocol	AODV

The complete scenario is divided into 4 clusters each containing 25 nodes. Each cluster having a head node via which communication takes place. The blue and red pair of nodes serves as wormhole nodes. They will cause the tunneling effect in the network and will further cause packet drop. Proposed scheme will defend against wormhole attack in the network. The final work is represented in the form of graph. End-to-End Delay is used for performance analysis.

End-to-end Delay: the average time taken by a data packet to arrive in the destination.

$$delay = \frac{\sum(arrive\ time - send\ time)}{\sum No.of\ connections}$$

Lower the value of end-to-end delay means the better performance of the protocol.

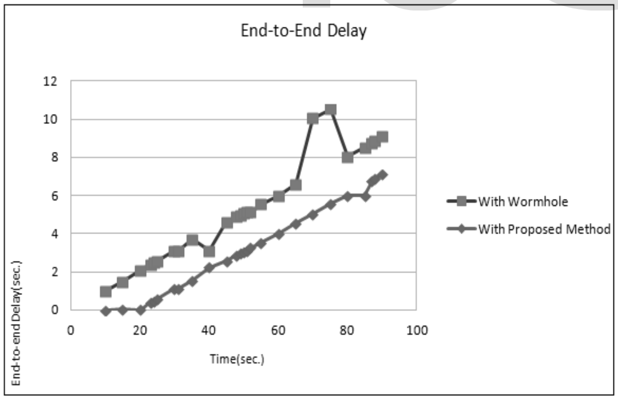


Figure 2: Impact of wormhole on End-to-End Delay and End-to -End Delay with proposed method

5. CONCLUSION

Wireless sensor networks is an emerging area as it has a great potential in various diverse areas, e.g., military, defense, disaster management, home applications, monitoring. However, it poses a great security risk in comparison to other conventional wireless networks. In this paper, we discuss wormhole attack problem which is a severe security risk in routing. We propose a simple, efficient and effective method to combat wormhole attack. The simulation results show effectiveness of the proposed method.

REFERENCES

[1] Hu Y C, Perrig A, et al. Packet leashes: a defense against wormhole attacks in wireless networks. 22nd Annual Joint Conference on the IEEE Computer and Communications Societies, Mar 30-April 3, 2003. San Francisco, CA, United States.

[2] Gajbhiye P, Mahajan A. A survey of architecture and node deployment in wireless sensor network. First International Conference on the Applications of Digital Information and Web Technologies, Aug 4–6, 2008: pp. 426-430

[3] Li Q, Zeng Q K. Efficiently detecting wormhole attacks in sensor networks by information potential. Third International Conference on Communications and Networking in China, Aug 25-27, 2008: 692-698

[4] E.A.Mary Anita et al. Defending against Wormhole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks, IEEE conference,2011:1-5

[5] Triki B, Rekhis S, Boudriga N. Digital investigation of wormhole attacks in wireless sensor networks. Eighth IEEE International Symposium on Network Computing and Applications, Jul 9-11, 2009:179-186

[6] S.K. Pramod, S. Govind. An efficient Prevention of Blackhole Problem in AODV Routing Protocol in MANET. 11th IEEE conference on Trust, Security and Privacy in Computing and Communication, 2011 902-906

[7] Bin T., Qi LI et al. A ranging based scheme for detecting the wormhole attack in wireless sensor networks. Sciencedirect, June 2012, 19(Suppl. 1): 6–10