ISSN 2320-9984
9 772320 998039 02

Volume 3 Issue 2 | June 2015 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

An Approach of AODV Protocol for the Intrusion Detection in the Mobile Adhoc Networks

Mayur M. Motwani
M. Tech (Scholar)
Department of Computer Science and Engineering
Lakshmi Narain College of Technology
Jabalpur (M.P.), [INDIA]
Email: mayur.motwani26@gmail.com

Sujeet Kumar Tiwari
Assistant Professor
Department of Computer Science and Engineering
Jabalpur (M.P.), [INDIA]
Email: Sujeet.tiwari08@gmail.com

Naazish Rahim
Head of the Department
Department of Computer Science and Engineering
Lakshmi Narain College of Technology
Jabalpur (M.P.), [INDIA]
Email: naazish . rahim786@gmail.com

Abstract**—***Wireless Sensor Networks (WSN) is a technology of trend now-a-days which has a large variety of applications such as battlefield surveillance, forest fire detection, traffic surveillance, flood detection etc. But wireless sensor networks are very much susceptible to a variety of potential attacks which disturbs the normal operation of the network. The Black hole attack is one of the dangerous security threat that affects the complete network from its normal functioning by completely advertising maliciously itself having shortest route to the destination and then tries to drop all the receiving packets. There are many mechanisms which have been proposed to defend network from the black hole attack, but none of the solution looks very effective to defend against the black hole attack. So in this paper, we have surveyed and compared the solutions to black hole attacks on AODV protocol. The Tabular representation of comparison depicts clear analysis of these solutions.*

Keywords:— *AODV, Black hole attack, IDS, Routing.*

1. INTRODUCTION

WSNs have wide application foreground in environmental monitoring, military, industrial control and other fields. These devices are used to collect information from the physical environment such as volcanic eruptions, tsunami and earthquake monitoring, and similarly, wildlife habitat monitoring, disaster management uses in battle field for tactical response team, weather monitoring, structural integrity monitoring, logistics, transportation, entertainment etc.

MANET are vulnerable to malicious attack because of its features like changing its topology dynamically, open medium, lack of central monitoring and management, cooperative algorithms and so on. These attacks are of many kinds such as snooping attacks, or wormhole attacks, routing table overflow and poisoning attacks, packet replication, black hole attacks, denial of service attacks(DoS), distributed DoS (DDoS) attacks etc. In the present paper we defined the black hole attacks in AODV routing protocol in mobile Ad-Hoc network. We use AODV

protocol as it is widely used and vulnerable to these attacks.

Ad-hoc Sensor Networks :

Infrastructure less*:* In this kind of network each and every node communicate with each other without any fixed infrastructure's communication overhead will not be more. Ad -hoc network don't require infrastructure.

Mobility: Mobility of nodes in ad-hoc networks more. The nodes are able to organize themselves in such a manner by exploring the area with out the presence of infrastructure they can communicate with each other.

Multi-Hoping: Ad-hoc Networks composed of several nodes and they are communicating with each other to describe several paths to several node. Here actually the packet traverses from one node to another node to reach the destination. Due to this Multi-hop features energy associated with each node can be conserved.

Openness: Ad-hoc network access information and services without geographic position.

Adaptability: Can freely adaptable to any situation and dynamically self-organize into arbitrary and temporary network topologies.

Heterogeneous Network: Ad-hoc network composed of heterogeneous devices like laptop, walkie-talkies etc. The different type of devices are able to communicate with each other.

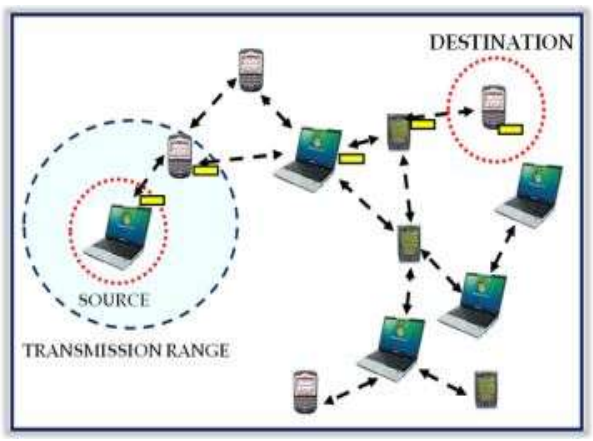

Figure 1.1 Mobile Adhoc Network

The applications are to be implemented for many applications, for example battlefield surveillance and monitoring the environment etc. But, the resource-constrained limitations make it essential for these sensor nodes to conserve energy to increase life-time of the WSN. An early aim was to use these kind of sensors in a way for indoor applications. These nodes had the capacity to sense the data such as temperature, humidity, pressure and location of the objects, which are surrounded in the environment. [Mani M. and Sharma A.K. 2012].

A wireless sensor network is a technology which emerged as a result of the advancement of network technology along with Micro Electro Mechanical Systems (MEMS). MEMS make it possible to design small size, low power sensors having communication and processing capabilities. Wireless sensor networks are mainly valuable in battlefield surveillance; environment monitoring, traffic monitoring and, weather and climate monitoring, detection of chemical or biological agent threats, and healthcare monitoring demand information gathering in harsh and inhospitable environments.

These applications require the usage of various equipment i.e. cameras and acoustic, infrared and seismic sensors for measuring different physical parameters. In a sensor networks nodes sense the information and transmit the collected data to base station through various paths such as direct and multi-hop. Actually, a WSN consist of hundreds to thousands of sensor nodes deployed in a random manner. Each of the sensor node is responsible for sensing the vicinity and transferring the sensed information to the Base Station (BS). Sensor nodes uses renewable energy sources so the energy optimization in WSN is a major issue. The architecture of wireless sensor network mainly consists of target region, sensor nodes, BS and user. [Bansal Komal, Sharma B.K., 2014]

Recently, there are lot of research efforts towards the optimization of standard communication paradigms for those networks.

Initially, these nodes had very less computation capacity and storage space and the only use was to transmit the scalar data to the base station (sink). The available sensor nodes have higher computation capacity, higher storage capacity and better power solutions with respect to their previous nodes and their primary usage area shifts from one indoor to another outdoor applications [Singh R., Gupta I. and Daniel A.K. 2014].

These sensor nodes have restricted computing and energy volume, thus protocols constructed for them must be simple, and energy efficient. These nodes consist of Communication unit (with receivers and transmitters), Processing unit, Power unit, Sensing unit and may also contain actuators for movement. Data sent to base station is collected periodically after short time intervals, via multi-hop routing mechanism. Main aim of Wireless Sensor Network is to detect events in dynamic environments, for object tracking and their classification. The network is designed to work without human support or maintenance, for several years, after deployment hence need to be robust, self-adaptive and should have healing capacity.

2. PROBLEM IDENTIFICATION

There are different kinds of attacks possible by malicious nodes to harm the network and make the network unreliable for communication and proper functioning. Some of theses kinds of attacks are:

a) ***Jamming:*** Jamming attack is related with disrupting or interfering the radio frequencies used by sensor nodes. Attacker may get physical access to some nodes and creates jam in the network to disrupt the network. Jamming attack come under physical layer attack.

b) ***Tampering:*** Refers to gaining the physical access to some set of sensors by tampering with their hardware configuration and making nodes to act as adversary node. Tampering is possible at physical layer.

c) ***Sybil Attack:*** Sybil attack is defined as a malicious device which takes on multiple identities. In Sybil attack an adversary can appear to be in multiple places at the same time. A single node presents multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of authenticated nodes. It is a Network layer attack.

d) ***Wormhole attack:*** Wormhole attack is an attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. This generates a false scenario that the original sender is in the neighbourhood of the remote location. The tunnelling forms wormholes in the sensor network. The tunneling or retransmitting of bits should be done selectively.

e) ***Hello Flood Attack:*** Hello flood attack is an attack which uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range (termed as a laptop-class attacker) and processing power, which sends HELLO packets to sensor nodes which are dispersed in a large area within a WSN.

f) ***Black hole:*** In Black hole attacks, a malicious node acts as a black hole to attract all the traffic in the sensor network through a node which is compromised or malicious node. A compromised node is placed at the center or any respective position, which looks attractive to neighboring nodes and attracts nearly all the traffic of surrounding nodes that was destined for a base station.

In this attack, a malicious node falsely advertises optimal paths to the destination node during the path-finding process (in reactive routing protocols), or in the route updates messages. The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the

destination node. A more delicate form of this attack is known as the grayhole attack, where the malicious node intermittently drops the data packets thereby making its detection even more difficult. Black hole attacks are classified into two categories:

- Single Black Hole Attack: In a single black hole attack there is only one node act as malicious or compromised node which misbehaves within the network. It is also known as black hole attack with single malicious node.
- Collaborative Black Hole Attack: In collaborative black hole attack multiple nodes behaves as malicious node in the network and work in co-operative manner. It is also known as the black hole attack with multiple malicious nodes.

3. RELATED WORK

DPRAODV (A Dynamic Learning System Against Black hole Attack in AODV Based MANET):

In this scheme, if the RREP sequence no. is greater than the threshold, the sender is referred as an attacker and updated to black list. An ALARM is sent to its neighbours who includes the black list to block malicious node. Whereas, On the other hand, the dynamic threshold value is changed by calculating the average of destination sequence number between the sequence number and that RREP packet in each time slot. In this, black hole is not only just detected but also prevented as updating threshold responses the realistic network environment.

In [8] and [9], the authors have introduced the route confirmation request (CREQ) and the route confirmation reply (CREP) to ignore and avoid the black hole attack. In this approach, the intermediate node not only is responsible for sending RREPs to the source node, but also it sends CREQs to the next-hop node toward the destination node. After receiving the CREQ, the next-hop node looks up its cache for some route to the destination. If it has a route, it sends the CREP to source node. After receiving the CREP, the source node confirms the validity of the path by comparing the path in RREP and CREP. If both the paths are matched, the source node judges that the route selected is correct. One demerit of this approach is that it cant avoid the black hole attack in which two consecutive nodes work in collision, that is, when next-hop node becomes a colluding attacker sending CREPs that support the incorrect path.

In [11], authors Satoshi Kurosawa et.al. have introduced an anomalous detection scheme to detect the black hole attack using a dynamic training method in which there is a training data, which is updated at regular intervals to express the state of the network. So, In this scheme, the average of the difference between the Destination in RREQ packet and the one which held in the list are calculated and this operation, which is executed for every received RREP packet. The average of this difference is finally computed for each timeslot and it is taken as the feature. Hence, it consumes considerable amount of time to perform all the calculations for every RREP packet.

In [12] Authors Ming-Yang Su et.al discussed a mechanism which is known as ABM (Anti-Black hole Mechanism), that is mainly used to compute the value of a node according to the amount of the abnormal difference between RREQs and RREPs transmitted and emitted from the node. When a suspicious value exceeds the limit, the nearest IDS broadcasts a block message with id of IDS, and the identified black hole node and the time of identification places the malicious nodes on their blacklists which isolates the malicious node in the network. The basic advantage of this method is that it is used to detect the cooperative black hole nodes in the MANETs. The main demerit of this technique is that the mobile nodes have to maintain an extra database for training the data and for its updation, in addition to the maintenance of their routing table.

In [13] this scheme, there is a trust based communication in MANET using AOMDV-IDS to prevent the black hole attack. AOMDV-IDS perform real time detection of attacks using the AOMDV routing protocol. In AOMDV, RREQ the transmission is from the source to the target, which establishes multiple reverse paths both at intermediary nodes and near the destination. Multiple RREPs navigates this reverse route back to and from multiple onward routes to the target at the source and intermediary nodes. These Multiple routes revealed are loop-free and disjoint. This Protocol depends on the routing information which is previously available in the AODV protocol, which prevents the overhead acquired in determining multiple paths.

In [14] authors Alem, Y.F et.al. proposed a solution, which is based on the Intrusion Detection using Anomaly Detection (IDAD) to prevent the attacks by the both single and multiple black hole nodes. IDAD assumes that every activity of a user can be watched and anomaly activities of an intruder can be identified easily from normal activities. To find a black hole node IDAD needs a pre-collected set of anomaly activities, called audit data. Once audit data is collected, it is given to the IDAD system, which compare every activity with audit data. If any activity of a node is out of the activity the listed in the audit data, the IDAD system isolates the particular node from the network. The reduction of the number of routing packets minimizes network overhead and facilitates a faster communication.

3. METHODOLOGY

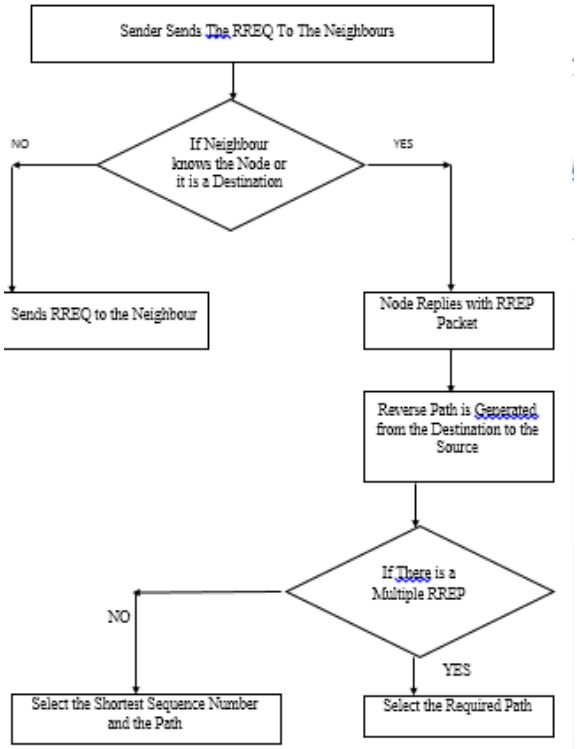

Figure 1: Flowchart of the Proposed Methodology

Step 1:- The Sender Sends the RREQ To The Neighbours

The Sender Node sends the route request which is commonly known as RREQ to the neighbouring nodes.

Step 2:- Determine If the Neighbouring node knows the Destination Node or not.

Check whether the node is the destination node or not

If not, Check whether it knows the destination node or not

If yes, the node replies with the RREP Packet giving the acknowledgement that it has received the node.

If no, then the Sender Node sends again the route request which is commonly known as RREQ to the neighbouring nodes.

Step 3:- Reverse Path Generation

When the node receives the reply, then the Reverse path will be gererated from the destination node or from the respective node.

Step 4 :- Computation of the Number of paths for the Path Generation.

There will be lot of paths from the Destination to source, but the comparison of all the paths will be necessary.

That's why the RREP and RREQ are compared to determine the shortest path

Step 5 :- Intrusion detection of the Path

If the comparison is done, and after comparison if the number of path varies, then the Intruser is detected.

As soon as the Intrusion detection is done, the Black Hole detection is done.

Step 6 :- Selection of Odd Man out

Select the Odd node out, and remove the node, so that the Path from the source to the destination is fixed.

Algorithm of The Methodology :-

Step 1 – send RREQ to the node

Step 2– monitor Each RREQ Packet from the Source to Destination.

Step 3 – compute the Number of various RREQ Path from Source to Destination.

Step 4 – destination Replies with RREP Packet

Step 5 – monitor RREP Packet

Step 6 – compute the Number of Reverse paths from the RREP Packet

Step 7 – compare Both the paths from RREP and RREQ

Step 8 – if the Number of path varies –

then

intruder Detected

select the odd node out

else

no intruder

4. RESULTS AND DISCUSSIONS

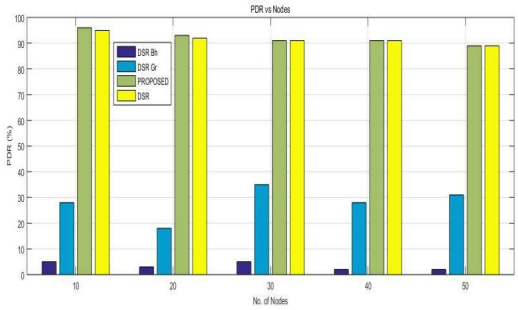

Figure 2: Shows the comparison of the DSR Bh, DSR Gr, DSR and the Proposed Approach

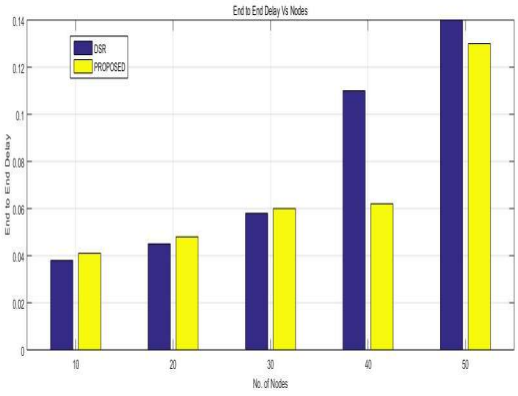

Figure 3: Comparison of End to end delay of nodes vs Number of nodes between DSR and Proposed Approach

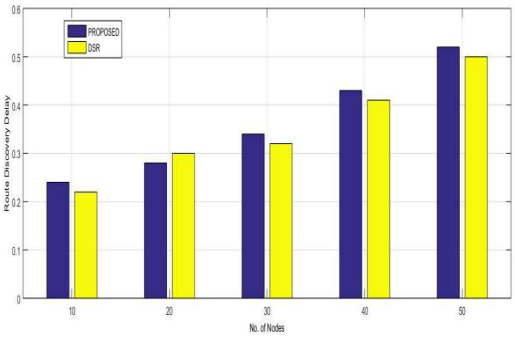

Figure 4 – Comparison of Route Discovery delay of nodes vs Number of nodes between DSR and Proposed Approach

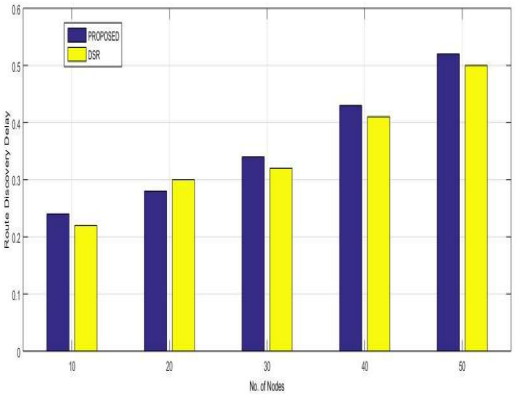

Figure 5: Comparison of use of data in MB, with respect to time in mili-seconds between DSR and Proposed approach

REFERENCES:

[1] J. Reynold, "Going Wi-Fi", Chapter 6, The Wi-Fi Standards Spelled out, Pg. 77http://www.cse.wustl.edu/~jain/cis788-99/adhoc_routing/index.html, 14 May 2006.

[2] T. Franklin, "Wireless Local Area Networks", Technical Reporthttp://www.jisc.ac.uk/uploaded_documents/WirelessLANTechRep.pdf. 25 July2005.

[3] P. Misra,. "Routing Protocols for Ad Hoc Mobile Wireless Networks",

[4] Webopedia, An Internet Dictionary, 14 May 2006 http://www.webopedia.com/TERM/T/Tcl.

[5] http://en.wikipedia.org/wiki/Personal_area_network, 25 July 2005.

[6] P. Yau and C. J. Mitchell, "Security Vulnerabilities in Adhoc Network".

[7] F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", December, 2004, http://masimum.dif.um.es/nsrt-howto/pdf/nsrthowto.pdf, 25 July 2005.

[8] H. Deng, W. Li and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October2002.

[9] K Fall and K. Varadhan, The NS Manual, November 18, 2005,http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf. 25 July 2005.

[10] D. Johnson, D. Maltz and J. Broch, "DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks". Ad Hoc networking, Chapter 5, page 139-172. Addison-Wesley, 2001.

[11] Virtual InterNetwork Testbed, http://www.isi.edu/nsnam/vint, 14 May 2006.

[12] NS by Example, http://nile.wpi.edu/NS/overview.html, 14 May 2006.

[13] C.Perkins, "(RFC) Request for Comments – 3561", Category: Experimental, Network, Working Group, July 2003.

[14] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Ad Hoc Networks", Proc. 6th Annual Int'l. Conf. Mobile Comp. and Net., Boston, MA. pp. 255 -265. August 2000.51

[15] P. Ning and K. Sun, "How to Misuse

AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols", Proc. of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003.

[16] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999. University of Cambridge Computer Laboratory.

[17] G. Vigna, S. Gwalani and K. Srinivasan, "An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks", Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04).

[18] http://certifications.wi-fi.org/ wbcs_certified_products.php 25 July 200.