Volume 2, Issue 3, July 2015 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Comparative Study and Analysis of Intrusion Detection Methods in Mobile Adhoc Networks

Mayur Motwani
M.Tech Scholar
Department of Computer Science and Engineering
Lakshmi Narain College of Technology
Jabalpur, (M.P.), [INDIA]
Email: mayurmotwani26@gmail.com

Sujeet Kumar Tiwari
Head of the Department
Department of Computer Science and Engineering
Lakshmi Narain College of Technology
Jabalpur, (M.P.), [INDIA]
Email: sujeet.tiwari08@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.*

I. INTRODUCTION

Wireless Sensor Network is a recently emerging technology consisting of a large number of distributed sensor devices which are used to collect the data from the environment. These devices have limited power in the terms of both energy and processing speed and also have low storage capacity. 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. each on the basis of mutual trust. MANET is normally used in military purpose, personal area network, disaster relief and so on. Every node communicates with the other which acts as routers. 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.

The Security in Mobile Ad-hoc Network is a very important aspect for the network. Therefore, there must be an efficient intrusion detection, which must be deployed to facilitate the identification and isolation of attacks. In this paper we have analysed various intrusion detection techniques in MANET against Black hole attack. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing.

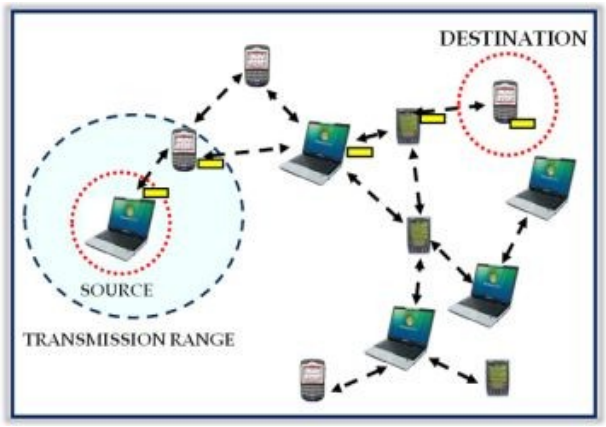

Figure 1 Mobile Adhoc Network

In the unstructured WSN, there are large numbers of nodes which are deployed randomly to monitor the region. Due to the unavailability of physical presence on that region, the network maintenance activities are very difficult. In the structured WSN, all the nodes are well deployed in a fixed and planned manner. Plus point of a structured network is that the fewer nodes can be deployed and they requires less maintenance and management cost. In a WSN, the object which is performing the task of sensing is called a sensor. Sensor nodes are very low power devices which are equipped with one or more sensors, memory, power supply, processor, a radio, and an actuator. A wide variety of mechanical power, biological, chemical, optical sensor thermal sensor, and magnetic sensors can be attached to increase the power of sensor nodes.. Since the sensor nodes have limited memory and are deployed in a very harsh environment and in difficult locations, radio transmitter is implemented just to transfer the collected data to base station. WSNs have many applications such as military target tracking and surveillance, health monitoring, disaster relief, environment exploration seismic sensing to measure the environment. Figure 1 shows the MANET model. The remainder of the paper is structured as follows.

II. 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 those 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 neighbor hood 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 gray hole 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.

III. Methodologies Used

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 details 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.

IV. CONCLUSION AND FUTURE WORK

Wireless Sensor Networks are thus very much vulnerable to many kinds of attacks due to the deployment of sensor nodes in an undisciplined environment. These types of networks suffers from the black hole attack because there is absence of centralized security management. This research paper provided a survey and analysis on the various countermeasures for the black hole attack. In this survey, we have given the security goals of a network. Then, we have presented some of the easiest possible network layer attacks in the Mobile Adhoc Networks. This survey also has the tabular analysis of various security procedures to prevent a particular network from the black hole attack. It is that this survey will really help the future researches in

Table 1: Analysis of the Methods Used and The result obtained in the research

Technique proposed by	Techniques	Type of black hole attack	Merits	Demerits	Routing Protocol
Payal N. Raj1 and Prashant B. Swadas2, 2008 [6].	Compares the RREP sequence numbers with threshold value using dynamic learning method	Single and multiple black hole	Increases PDR with Minimum increase in Average end-to end delay	Higher Routing overhead and can't detect cooperative black holes	AODV
Y.Zhang and W.Lee,2000 [8]	introduces the CREQ and CREP to avoid black hole	Single black hole	Low cost	Time delay and false positives	AODV
Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Nov. 2007 [11].	A new detection method based on dynamically updated training data.	Single black hole	Detection rate and false positive rate improve	Network delay	AODV
Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, Sept. 2010 [12].	An Anti-Black hole Mechanism (ABM) using IDS	Multiple black holes	High detection rate	Time delay	AODV
Akanksha Jainapril 2012 [13]	Trust based communication using AOMDV_IDS	Single black hole	Minimum overhead	Poor performance of network due to Routing overhead increases	AODV
Alem, Y.F.; Zhao Cheng Xuan; May 2010 [14]	Intrusion detection using anomaly detection (IDAD)	Single and multiple black hole nodes	Minimum network overhead	Neighbour nodes may give false information	AODV

developing a good knowledge about the Intruder attacks and their countermeasures.

REFERENCES:

[1] Arunmozhi, S. A., and Y. Venkataramani. "Black Hole Attack Detection and Performance Improvement in Mobile Ad-Hoc Network." Information Security Journal: A Global Perspective 21, no. 3 (2012): 150-158.

[2] Tanuja, R., M. K. Rekha, S. H. Manjula, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik. "Elimination of black hole and false data injection attacks in wireless sensor networks." In Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, pp. 475-482. Springer New York, 2013.

[3] Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, 28-30 December 2001

[4] Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Paper presented at the ACM SIGCOMM'94 Conference, London, United Kingdom, August 31 -

September 2, 1994.

[5] Tamilarasan-Santhamurthy;"A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols in MANET", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011, PP: 176-184.ISSN (online):1694-0814.

[6] Noman Mohammed, HadiOtrok, Lingyu Wang, MouradDebbabi and Prabir Bhattacharya "Mechanism Design Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

[7] Raj PN, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET", International Journal of Computer Science 2: 54-59, 2009.

[8] Y.Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks", 6th annual international Mobile computing and networking conference proceedings, 2000.

[9] Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks" 2002, international Conference.

[10] Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by YibeltalFantahumAlem& Zhao HhengXaun from Tainjin 300222, China 2010, IEEE.

[11] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[12] Ming-Yang Su; Kun-Lin Chiang; Wei -Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.Lee J.S. and Cheng W.L. September 2012. "Fuzzy-Logic-Based Clustering Approach for Wireless Sensor Networks Using Energy Predication", IEEE Sensors Journal, vol. 12, no 9, pp. 2891-2897,.

[13] Dechene D.J, Jardali A.E., Luccini M., and Sauer A. 2012, "A Survey of Clustering Algorithms for Wireless Sensor Networks", Department of Electrical and Computer Engineering, The University Of Western Ontario, London, Ontario, Canada.

[14] Verdone R.,DardariD., Mazzini G., and Conti A. 2010, Wireless sensor and actuator networks: technologies, analysis and design. Academic Press.

[15] Yang, B.; Xu, J.; Yang, J.; Yang, D. 2010 A novel weighted clustering algorithm in mobile ad hoc networks using discrete particle swarm optimization. Int. J. Network. Management, 20, 71-84.

[16] Aries K. and Kyung, O.L. 2011 "A clustering protocol with mode selection for wireless sensor network," Journal of Information Processing Systems, vol. 7, No. 1, pp.29-41.

[17] Liu B., Pei B.N., Chen W.W. and Yang Z.F 2011, "Improved clustering routing algorithm based on energy control of cluster-heads," Computer Engineering and Applications, vol. 47, No.12, pp.69-71.

* * * * *