Proc. of Int. Conf. on Emerging Trends in Engineering & Technology, IETET

Survey of AODV Black Hole Attack using WSN

Akshay Kansra[1] and Ankur Singhal[2]
[1]Geeta Institute of Management and Technology, Kurukshetra, India
Email: akshay.kansra@gmail.com
[2]Geeta Institute of Management and Technology, Kurukshetra, India
Email: ankursinghal@gimtkkr.com

***Abstract*—Wireless sensor network (WSN) has various field of applications, but on the other hand it is at high level to the various security threats. These networks are easily leveled to security attacks, since once deployed these networks are unattended and unprotected. Some of the inbuilt features like limited battery and low memory makes sensor networks are infeasible to use predictable security solutions, which needs complex computations and high memory. There are number of attacks on wireless sensor networks similar to black hole attack, selective forwarding attacks, sink hole attack, Sybil attack etc. This paper present work on the wireless sensor network in the existence of black hole attackers using Ad-hoc on Demand Distance Vector Routing Protocol. The black hole type of attacker node absorbs every message passing through it. So the precious node attacks the whole traffic in the network.**

***Index Terms*— WSN, AODV, Attack,Black Hole Attack.**

I. INTRODUCTION

Wireless sensor networks (WSN) become popular from the academia to industry[1] in recent years due to their broad range of application , such as object localization or tracking, environmental monitoring, scientific exploration in dangerous environments and so forth, In particular, many applications require global time synchronization, that is, all the nodes of the network achieve and maintain a common notion of time for most sensor network applications, the data received are meaningless and useless without time and space information of an event. The accurate time synchronization is required in many circumstances in network applications. For example, media access control layer of IOS using TDMA needs correct time information, so that transmissions of signal do not interfere; the sleep scheduling needs nodes to sleep and wake up at the same time. In addition, some special application such as mobile goal localization and event detection also need synchronization. Sensor nodes are randomly distributed within the target area and form a cluster-based network by LEACH protocol architecture for micro sensor networks. LEACH includes some distributed cluster formation techniques whichallows self-organization of huge numbers of nodes, and algorithms for adapting clusters and rotating cluster-head election to distribute energy load among all the nodes. After the cluster-heads are elected, the clusters overlap each other through the power control nodes in the overlapping region are called overlap-nodes.

A. Wireless Sensor Network

In recent years, applications of WSNs have been increased due to its vast possible to connect the physical

Grenze ID: 02.IETET.2016.5.22

world with the virtual world. Advancement in microelectronic fabrication technology reduces the cost of production of portable wireless sensor nodes. It becomes an ease to use the large numbers of portable wireless sensors in wireless sensor network to increase the quality of service. The QoS of such WSNs is mainly affected by the failure of sensor nodes prospect of sensor node failure enhances with increase in number of sensors. In order to uphold the better quality of service under failure conditions, reorganization and disconnection such faults are essential. The WSN may fail due to a range of reasons, including the following: the routing path might experience a break; the WSN sensing area might experience a leak; the battery of some sensor nodes might be depleted, requiring more relay nodes; or the nodes wear out after the Wireless Sensor Network has been in use a long period of time [4].

B. AODV Routing Protocol

AODV means Ad-hoc On-Demand Distance Vector is an on demand routing protocol which is used to find a route from source to destination node as needed. For establishing a path from the source to the destination it uses control messages such as RREQ and Route Reply (RREP). Header information of these control messages [7] are described in fig 1 & 2. If a source node wants to make a link with the destination node, it broadcasts an RREQ message to its neighbors. This RREQ message is propagated from the source and received by its neighbors (intermediate nodes) of the source node. Neighbor nodes get the RREQ from the intermediate nodes to communicate. This iteration continues until the packet is taken by destination node or an in between node that has a fresh route entry for the destinations in its routing table. Fresh enough means that its intermediate node has a valid route to the destination confirmed earlier than a time period set as a threshold [8]. By using RREQ from an in between node rather than the destination node reduces the route establishment time and also the traffic control in the network.

Source Address	Source Sequence	Destination Sequence	Broadcast Address	Destination Address

Figure 1. Frame format of RREQ

Source Address	Destination Address	Destination Sequence	Hop Count

Figure 2. Frame format of RREP

II. Black Hole Attack in AODV

Two types of black hole attack can be considered in AODV in order to distinguish the kind of black hole attack:

A. Internal Black Hole Attack

These attacks have an internal malicious node which fits in intermediate routes of given source and destination [1]. As soon as it gets the chance this malicious node generate itself an active data route element. At this stage it is capable of conducting attack with the start of data transmission [2]. This attacks because node itself belongs to the data route. Mitigation of internal attack is more difficult because of complexity in detecting the internal misbehaving node.

B. External Black Hole Attack

These attacks physically stay exterior of the network and oppose access to network traffic or creating congestions in network or by disrupting the entire network [3]. External attack can become a kind of internal attack when it takes control of internal malicious nodes and control it to attack other nodes in WSN. External black hole attack can be summarized in following points [4]. • Malicious node detects the dynamic route and notes the destination address. Malicious node sends a route reply packet (RREP) as well as the destination address field spoofed to an unknown address. Hop count value is set to lowest rate and the sequence number is set to the highest value. • Malicious node sends RREP to the nearest available node which belongs to the active route to destination. This can also be send directly to the data source node if route is available. • The RREP established by the nearest node to the malicious node will relayed via the established opposite route to the data of source node. • The new information received in the route reply will allow the source node to

inform its routing table. • New route selected by source node is used for selecting data. • The malicious node will drop now all the data to which it goes in the route.

III. Security Threat

With the increased use of computers and ease of way in to internet, the ways to attack and cheat a system has also increased [7].

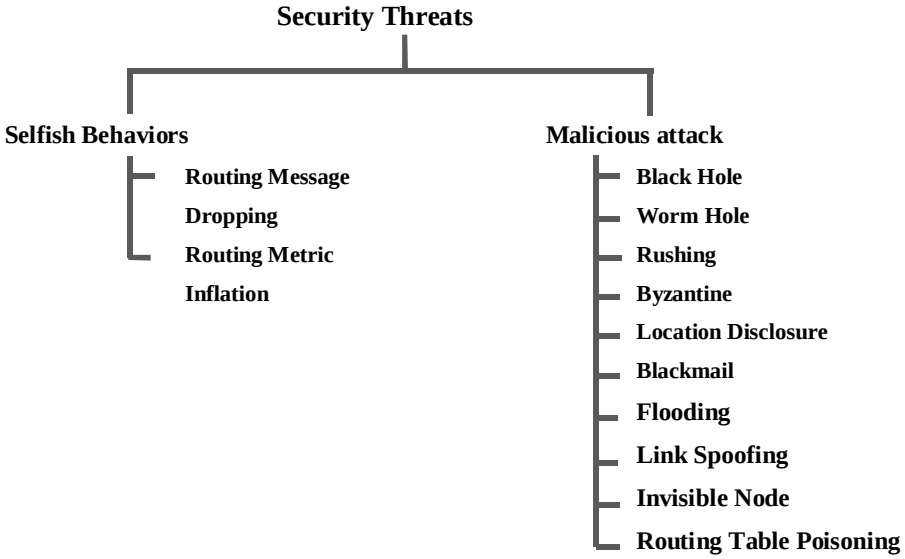

Figure 3. Types of Security Threads

A. Black hole

First, the malicious node attracts traffic through itself by advertising better routes to the requested destinations. Afterward, the malicious node drops all the data or control packets progress through it without any forwarding.

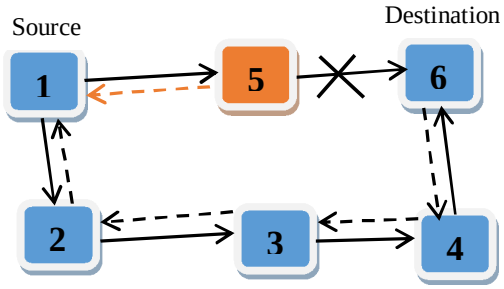

Figure 4.Black Hole

B. Wormhole

A malicious node apprehends packets from one location in a network and passes them through an out-of-band channel to another malicious node [10] located several hops away, which replays them to its neighboring nodes, the tunnel between the malicious nodes is faster than links between legitimate nodes, so the tunneled packets arrive faster than packets through other routes. Therefore, the malicious nodes are more likely to be included in the route and take an edge for future attack.Detection of wormhole attack is generally difficult, and requires the use of an immutable and individualistic physical metric, such as time delay or geographical site.

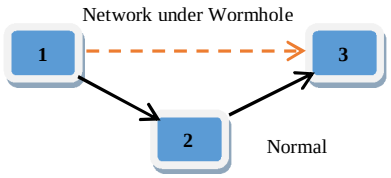

Figure 5.Warm Hole Attack

C. Rushing

This attack can be carried out by opposing on-demand routing protocols that use duplicate suppression in their operations. In order to reduce the route discovery overhead, each intermediate node processes only the first received route request packets and rejects any duplicate packets that arrive later. Rushing node exploits this mechanism by disseminating route request packets in order to be included in the discovered routes. Rushing attack can be performed in many ways: by transmitting at a higher wireless transmission power level, by ignoring delays at MAC or routing layers, by keeping other nodes' transmission queues full or by using a wormhole tunnel.

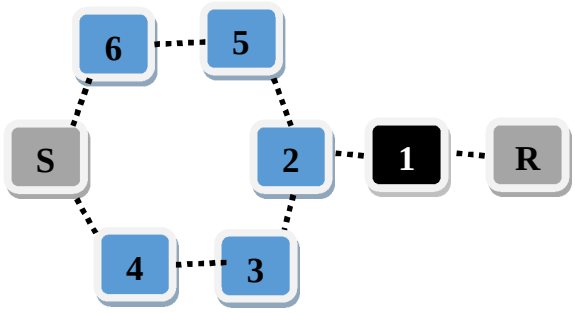

Figure 6. Rushing Attack Near the Receiver

D. Byzantine

A malicious node or a group of malicious nodes create or modify control packets with false routing information in order to disrupt or degrade the routing operation. This attack
is not easy to detect because it has not a specific form; the malicious node can create routing loops, drops or diverts packets to non-optimal routes.

E. Location disclosure

Location disclosure is an attack that aims the privacy attribute of an ad hoc network. A malicious node can reveal important information such as location of nodes, or even the structure of the entire network, by the use of traffic analysis techniques, or with simpler probing [9] and monitoring approaches. Colluding nodes may gather information regarding the identities of communication parties; analyze traffic to learn the network traffic pattern, track changes in the traffic pattern, and then plans further attack scenarios. The leakage of such information is destructive in security sensitive scenarios.

F. Blackmail

This attack occurs against routing protocols that employs malicious detection mechanisms like Watchdog and path rater. Malicious node may exploit these mechanisms to blackmail legitimate nodes in order to incite other legitimate nodes to put those legitimate nodes in their blacklists.

G. Link spoofing

In this attack, a malicious node announces fiction links with non-neighbor's node. The Optimized Link State Routing protocol OLSR constitutes a typical example for this attack, where malicious node can convince a victim node to select him as an MPR by advertising fake links with the target's two-hop neighbors.

H. Invisible node

This attack happens when a malicious node M situated at the same time in the range of two legitimate nodes T1 and T2, knowing that T1 and T2 are not directly reachable by each other. By broadcasting the control messages from T1 to T2 and vice versa, the malicious node A arrives to create an inexistent physical link between T1 andT2, which can fully control and can break at any time it wants. The detection of this attack is very difficult since them malicious node do not alter the broadcast messages. Basically, this attack targets proactive routing protocols. Malicious node forges route to non-existent destination, and then floods these bogus routes in excessive route advertisements to overflow the neighbor's routing table. The goal of this attack is to have enough routes so that creation of new routes is halted or the implementation of routing protocol is overwhelmed.

I. Routing table poisoning

Due to promiscuous mode, [5] in which a node can update its routing table with the routing information hold in the packets that it overhears, malicious node may poison routes to a victim node(s), by generating and sending fabricated routing packets, or by modifying legitimate packets from other nodes, in order to create erroneous entries in the routing tables of the participating nodes. This attack can cause the creation of routing loops, partition network or the selection of non-optimal routes.

IV. CONCLUSION

Safe and on time broadcast of packets is the basic need in wireless sensor network. One of the attacks that violate this requires Selective forwarding attack. In this attack, a malicious node is falling packets which makes information unavailable. We have discussed some of the reduction schemes to defend this attack and had given analysis on every scheme.

REFERENCES

[1] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[2] Ashfaq Hussain Farooqi, Farrukh Aslam Khan, Jin Wang, Sung Young Lee, "a Novel intrusion detection frame work for wireless sensor network", Personal and Ubiquitous Computing Springer journal (DOI 10.1007/s00779-012-0529-y), pp. 907-919, June 2012.

[3] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", Proceedings of the 33rd IEEE Conference on Local Computer Networks (LCN), Dublin, Ireland, pp. 76-83, October 2007.

[4] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks", Proceedings of the ACM workshop on Wireless security. New York, USA, pp. 41–50, 2003.

[5] Amara korbaAbdelaziz, Mehdi Nafaa "Surveyof Routing Attacks and Countermeasures in Mobile Ad Hoc Networks" IEEE 2013.

[6] R. Ramanujan, A. Ahmad, J. Bonny, R. Hagelstrom, K.Thurber, "Techniques for Intrusion-Resistant Adhoc Routing Algorithms (TIARA)", MIL-COM 2000, 21st century military communications conference proceedings, pp. 660-664, 2000

[7] Sheela.D, Srividhya.V.R, AsmaBegam, Anjali and Chidanand G.M,Detecting Black Hole Attack in Wireless Sensor Network using Mobile Agent, Proceedings of International Conference on Artificial Intelligence and Embedded Systems Singapore, pp 45-48 July 2012.

[8] Saurabhgupta, SubratKar, S. Dharmraja, "Black Hole Attack Avoidance for Wireless Adhoc Network", International Conference On Computer & Communication Technology (ICCCT)-2011

[9] Ming Yang Su, Kun Lin Chiang, Wei-Cheng Liao, "Mitigation of Black Hole Nodes in Mobile Adhoc Networks", IEEE, 2010

[10] WatcharaSaetang and SakunaCharoenpanyasak "CAODV Free Black Hole Attack in Mobile Adhoc Networks" International Conference on Computer Networks and Communication Systems, vol.35 (2012), Singapore

[11] HesiriWeerasinghe and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Intention Journal of Software Engineering and its Application, Vol.2, Issue 3, July 2008.