Volume 5, Issue 4, April 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Jamming attack in MANET: A Selected Review

[1]Baljinder Singh, [2]Dinesh Kumar

[1]Student Masters of Technology Department of CSE,GZS-PTU Campus,Bathinda,Punjab, india

[2]Associate Professor, Department of CSE, GZS-PTU Campus,Bathinda,Punjab, india

Abstract---A MANET is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected Wireless sensor networks are being used in many applications like health monitoring, military purposes, and home automation. 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. This paper reviews security issues on Ad-hoc network and Ad hoc On-Demand Distance Vector (AODV) protocol. In Ad-hoc network, active attack i.e. DDOS, black hole attack, wormhole attack, jamming attack can easily occur. These attacks can decrease the performance of the communications protocol. The given paper gives the comprehensive review of Jamming attack and its features in different techniques. Every technique has its own merits and demerits. We study various techniques related to Jamming attack and here presents few basic techniques for review.

Keywords---Mobile Ad Hoc Network; AODV Protocol; Jamming Attack; Wireless sensor networks

I. INTRODUCTION

Wireless networks have paved the way for mobile nodes to communicate with each other. The two basic system models are fixed backbone wireless system and wireless Mobile Ad hoc Network (MANET).[2][3] A MANET is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. Therefore the functioning of ad hoc networks is dependent on the co-operation of each and every node. The nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. The rapid proliferation of wireless ad-hoc networks and mobile computing applications has changed the landscape of network security. Wireless networks are networks which provide users with connectivity regardless of their actual physical location. WSN's (Wireless sensor Networks) are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. [6]

1.1 MAJOR ATTACKS ON MOBILE AD HOC NETWORKS

A) Black Hole: -

MANETs are vulnerable to various attacks among them the black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path by sending fake RREP with higher sequence number to the source node in order to pretend like a destination node, so, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself, due to this actual source and destination nodes are unable to communicate .It drops the packets or do not allows forwarding of packets to neighbors. This attack is known as black hole as it swallows the data packets.

B) Gray-hole: -

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are:-

- Dropping all UDP packets while forwarding TCP packets and another may be Dropping 50% of the distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.
- Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are:-

• Dropping all UDP packets while forwarding TCP packets and another may be Dropping 50% of the distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.

• Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

C) Wormhole:-

A wormhole attack is considered dangerous as it is independent of Mac Layer. Wormhole attack is also known by name of tunneling attack. It specifically consider Tunneling attack which does not require exploiting any nodes in the network and can interfere with the route establishment process by capturing packet from one point in the network, and tunnels the recorded packets to another point which is a malicious node and later on packets in the network can be transmitted again locally .In wireless ad hoc networks, it is difficult to trace out wormhole attacks because malicious nodes behaves as legitimate nodes.

D) Jamming Attack: -

It is a type of DOS attack. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications. Some possible strategies are exposed below:

• *Constant Jammer*: A constant jammer continuously emits a radio signal that represents random bits; the signal generator does not follow any MAC protocol.

• *Deceptive Jammer*: Different from the continuous jammers, deceptive jammers do not transmit random bits instead they transmit semi-valid packets. This means that the packet header is valid but the payload is useless.

• *Random Jammer*: Alternates between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), and in the second mode (the sleeping mode) the jammer turns its transmitters off for another random period of time. The energy efficiency is determined as the ratio of the length of the jamming period over the length of the sleeping period.

• *Reactive Jammer:* A reactive jammer tries not to waste resources by only jamming when it senses that somebody is transmitting. Its target is not the sender but the receiver, trying to input as much noise as possible in the packet to modify as many bits as possible given that only a minimum amount of power is required to modify enough bits so that when a checksum is performed over that packet at the receiver it will be classified as not valid and therefore discarded.

II. LITERATURE REVIEW

2.1 Improving Reliability of Jamming Attack Detection in Ad hoc Networks [4]

Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar represent this technique in 2011

In this work, they focused on jamming type DoS attacks at the physical and MAC layers in 802.11 based ad hoc networks. Collisions in wireless networks occur due to varying factors such as jamming attacks, hidden terminal interferences and network congestion. The author presented a probabilistic analysis to show that collision occurrence alone cannot be used to conclusively determine jamming attacks in wireless channel. To increase the reliability of attack detection, it was necessary to provide enhanced detection mechanisms that must determine the actual cause of channel collisions. To address this, they first investigate the problem of diagnosing the presence of jamming in ad hoc networks. Then they evaluate the detection mechanism using cross-layer information obtained from physical and link layers to differentiate between jamming and congested network scenarios. By correlating the cross-layer data with collision detection metrics, they might distinguish attack scenarios from the impact of traffic load on network behavior. Through simulation results the author demonstrated the effectiveness of the proposed scheme in detecting jamming with improved precision.

2.2 Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks [8]

Kwangsung Ju and Kwangsue Chung represent this technique in 2012

In a tactical field, wireless communication is prevailed among military agents and vehicles, but it is fragile by jamming attack from an adversary because of the wireless shared medium. Jamming attack is easily achieved by emitting continuous radio signal and it can interfere with other radio communications within the network. Channel switching over multiple channels or route detouring have been proposed to restore communication from jamming attacks, but they require a special radio system or knowledge of network topology. In this paper, in order to overcome limitations of the previous research, the author proposed a new robust rate adaptation scheme that was resilient to jamming attack in a wireless multi-hop tactical network. The proposed rate adaptation scheme detects jamming attack and selects the data transmission mode which had the expected maximum throughput based on the successful transmission probability. Through the performance evaluations, they prove rate adaptation scheme that improved packet delivery ratio and the wireless link utilization.

2.3 All Your Jammers Belong To Us - Localization of Wireless Sensors under Jamming Attack [9]

Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague represent this technique in 2012

In this paper, the author proposed an approach to localize a wireless node by using jamming attack as the advantage of the network. The proposed localization technique was divided into two steps. First, they discover the location of the jammer using power adaptation techniques. Then, they use these properties to extrapolate the locations of jammed nodes. Furthermore, the author design a localization protocol using this technique, and demonstrated the feasibility of the proposed mechanism by conducting indoor experiments based on IEEE 802.15.4 wireless nodes. The proposed result shows that for some situations the proposed mechanism might be used to locate mobile nodes under jamming attack.

2.4 SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks [11]

Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi represent this technique in 2013

In this paper, the author presented SAD-SJ, a self-adaptive and decentralized MAC-layer solution against selective jamming in TDMA-based WSNs. SAD-SJ does not need a central entity, requires sensor nodes to rely only on local information, and allows them to join and leave the network without hindering other nodes activity. They showed that SAD-SJ introduce a limited overhead, in terms of computation, communication and energy consumption. The proposed solution neutralizes the selective jamming attack, by forcing the adversary to perform a random attack, thus reducing its effectiveness to 1/*N*, where *N* is the total number of slots in the superframe. Moreover they had shown that SAD-SJ was self adaptive, as it allowed nodes to join and leave the network at any time and without affecting security of other nodes. Finally, SAD-SJ displayed a negligible impact on network performance, and results in an additional energy consumption which was limited and affordable

2.5 Self-Healing Wireless Networks under Insider Jamming Attacks [12]

Longquan Li, Sencun Zhu, Don Torrieri, Sushil Jajodia represents this technique in 2014

In this work, the author tackled the jamming attack problem in a systematic way. Specifically, they design a protocol that was capable of self-healing wireless networks under jamming attacks. The protocol identified and excluded an insider jammer and then restores normal data communications among benign nodes despite the presence of jamming by an initially unknown compromised node. The proposed scheme integrate key management, jammer identification and jammer isolation in one system. Finally, they evaluated the protocol with USRP devices and GNU Radio in the context of jammer localization. The experiments showed that the proposed protocol must identify and isolate the insider jammer with high accuracy.

III. COMPARATIVE ANALYSIS OF RESEARCH WORK

Sr.No.	Author/Research Study-Year	Title	Technology/ Methods	Results/Conclusion
1.	Geethapriya Thamilarasu , Sumita Mishra and Ramalingam Sridhar/ IJCNIS 2011	Improving Reliability of Jamming Attack Detection in Ad hoc Networks	Cross Layer Technique	Ease to detect Attacks with enhanced reliability and accuracy.
2.	Kwangsung Ju and Kwangsue Chung/ IJSIA 2012	Jamming Attack Detection and Rate Adaption Scheme for IEEE 802.11 Multi-hop Tactical Networks	Rate Adaptation	Improve packet delivery ratio and the wireless link utilization.
3.	Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague/ IEEE 2012	All Your Jammers Belong To Us - Localization of Wireless Sensors Under Jamming Attack	Localization Technique	By conducting Indoor experiments with IEEE 802.15.4 wireless nodes, the proposed approach was accurate and feasible.
4.	Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi/ IEEE 2013	SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks	SAD-SJ	Limited overhead, in terms of computation, communication and energy consumption
5.	Longquan Li, Sencun Zhu, Don Torrieri, Sushil Jajodia/ IEEE 2014	Self-Healing Wireless Networks under Insider Jamming Attacks	Self Healing	Integrates key management, jammer identification and jammer isolation in one system

IV. PROPOSED WORK

The proposed work mainly deals with the survey of different types of attacks in MANETS. The paper contains the cause of various major attacks and their functionalities. In this paper, we mainly compare the effect of wormhole attack and black hole attack in AODV routing protocol. The comparison will be evaluated for throughput of the network.

V. CONCLUSION

Nowadays, Security is a critical issue in the field of computer networks. They are more vulnerable to attacks and we have improved the quality and issues in Mobile Ad-hoc network and routing protocols. As jamming is a very serious threat to the normal operation of wireless networks, recently much research has been done to deal with it. All techniques are good from their point of view but not best from all points. Techniques discussed in this paper that can provide knowledge about security functions and an overall visual check, which might be suitable in some applications. But, there is also need to simulate a particular scenario to visualize the effect of with and without Jamming attack for the enhanced routing protocol.

REFERENCES

[1] Anthony D. Wood and John A. Stankovic(2004), “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks”, IEEE

[2] Ashish Kumar Jain, Vrinda Tokekar(2011), “Classification of Denial of Service Attacks in Mobile Ad Hoc Networks”, IEEE, pp.no-256-261.

[3] Dressler, F. (2008),"A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks” Elsevier Computer Communications, vol. 31 (13), pp. 3018-3029.

[4] Geethapriya Thamilarasu , Sumita Mishra and Ramalingam Sridhar(2011), "Improving Reliability of Jamming Attack Detection in Ad hoc Networks", IJCNIS, vol.3, no.1.

[5] Hong Huang, Nihal Ahmed, and Pappu Karthik(2011), “On a New Type of Denial of Service Attack in Wireless Networks:The Distributed Jammer Network”, IEEE, , VOL. 10, NO. 7.

[6] Manasi Sarkar, Debdutta Barman Roy(2011), “Prevention of Sleep Deprivation Attacks using clustering”, IEEE, pp.no- 391-394.

[7] Mohammed BOUHORMA, H. BENTAOUIT, A.BOUDHIR(2009), “Performance Comparison of Ad-hoc Routing Protocols AODV and DSR”, IEEE.

[8] Kwangsung Ju and Kwangsue Chung(2012), "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks", IJSIA, vol. 6, no. 2.

[9] Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague(2012), "All Your Jammers Belong To Us - Localization of Wireless Sensors Under Jamming Attack", IEEE.

[10] Selvamani K, Anbuchelian S, Kanimozhi S, Elakkiya R, Kannan A(2012), “A Hybrid Framework of Intrusion Detection System for Resource Consumption Based Attacks in Wireless Ad-Hoc Networks”, IEEE.

[11] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi(2013), "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", IEEE

[12] Longquan Li, Sencun Zhu, Don Torrieri*y*, Sushil Jajodia(2014), "Self-Healing Wireless Networks under Insider Jamming Attacks", IEEE

[13] G.Mahalakshmi, Dr.P.Subathra(2014), “A Survey on Prevention Approaches for Denial of Sleep Attacks in Wireless Networks”, JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, vol-6, no1.

[14] Kasturiniva Das, Amar Taggu(2014),“A Comprehensive Analysis of DoS Attacks in Mobile Adhoc Networks”, IEEE, pp. no- 2273-2278.