International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 410-414
e-ISSN:2278-621X

SURVEY ON JAMMING ATTACK IN MANET

Dylan Fernendes[1] & Rakesh Kumar B[2]

Abstract - A MANET is a group of nodes that do not depend on a pre-specified infrastructure to hold the network linked Wireless sensor networks are being utilized in some applications i.e. military purposes, health monitoring, and home automation. These networks are fitted with huge no. of sensors, which are spatially distributed. WSNs are broadly utilized in remote fields, defence and military scenarios. Thus, their security is serious problem. They are more susceptible to attacks as compared to wired networks. Wireless sensor networks endure from several active and passive attacks. This paper surveys security problems on Ad-hoc network and Ad hoc On-Demand Distance Vector (AODV) protocol. In Ad-hoc network, active attack such as DDOS, wormhole attack, black hole attack, jamming attack can easily happen. These attacks can reduce the communications protocol performance. The provided paper offers the comprehensive survey of Jamming attack and its characteristics in various techniques. Also, various techniques of Jamming attacks are studied understand the strengths and weaknesses.

Keywords - Mobile Ad Hoc Network, Jamming attack, AODV Protocol, Wireless sensor networks

1. INTRODUCTION

Wireless networks have covered the way for mobile nodes to interact with one another. The two basic system models are static backbone wireless system and wireless Mobile Ad hoc Network (MANET).[1][2] A MANET is a set of nodes that do not depend on a pre-specified infrastructure to hold the network linked. Thus, the services of ad hoc networks are based on the co-operation of each and every node. The nodes support each other in carryinginformation about the network configuration and share the responsibility of maintaining the network. The fast proliferation of mobile computing applications and wireless ad-hoc networks has changed the network security landscape. Wireless networks are networks that offer subscribers with connectivity without regarding of their actual physical position.

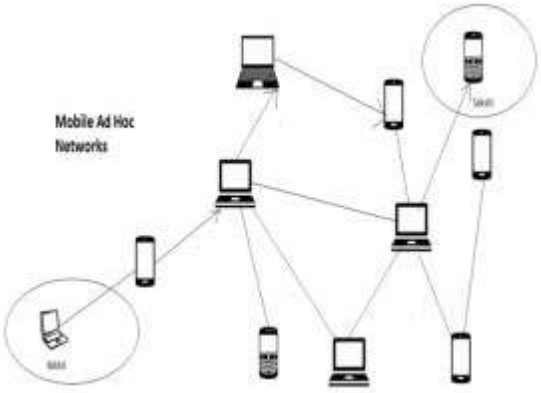

Fig 1. Mobile Ad Hoc Networks

Mobile Ad Hoc Networks (MANETs) has become one of the most significant areas of research in the last few years due to the challenges it introduces to the related protocols. MANET is the novel evolving technique that enables subscribers to interact without any physical infrastructure without regarding of their geographical position, thus it is sometimes known as an ―infrastructure less‖ network. The development of small, cheaper and more powerful devices build MANET a fastest developing network. An ad-hoc network is self- adaptive and self-organizing. Mobile ad hoc network devices should be capable to determine the existence of other devices and perform essential set up to provide communication and sharing of service and data. Ad hoc networking permits the devices to manage links to the network as well as easily joining and discarding devices to and from the network. Because of node mobility, the network configuration may change frequently and unpredictably throughout time.

2. ROUTING PROTOCOLS

Routing is the way towards transmitting data or packets from source node to goal node. As Ad-Hoc network changes their topology every now and again and in this manner making packet routing troublesome at that moment. Routing protocol

[1] Department of Computer Science, AIMIT, St. Aloysius College, Mangalore, Karnataka, India
[2] Assistant Professor, Department of Computer Science, AIMIT, St. Aloysius College, Mangalore, Karnataka, India

controls the stream of information in systems and furthermore chooses the efficient way to achieve the goal. Routing protocols can be categorized on various bases such as on the topology of network for routing i.e. proactive and reactive routing protocols, on the basis of communication strategy used for transmitting of information from source to destination i.e. unicast, broadcast and multicast routing [3]. Routing protocols define a set of rules which governs the strategy of message packets transfer from source to destination in a network [4].

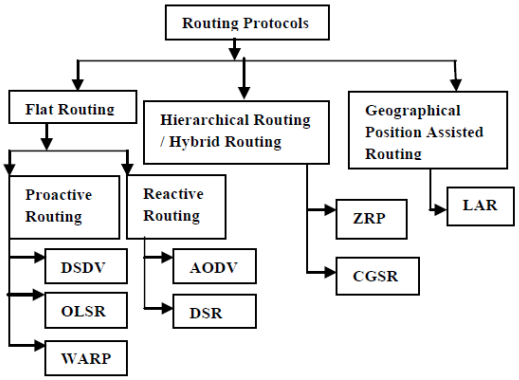

Fig 2. Classification of MANET Routing

2.1 Proactive (Table-Driven)

The pro-active routing protocols [5][6] are similar to current Internet routing protocols i.e. DV(distance-vector), the RIP(Routing Information Protocol), OSPF (Open Shortest Path First) and link-state. They try to manage up to date and consistent routing information of the entire network. Every node has to manage one or more tables to save routing information, and reply to changes in network configuration by flooding and propagating. Some available pro-active ad hoc routing protocols are : WRP (Wireless Routing Protocol, 1996), DSDV (Destination Sequenced Distance-Vector, 1994), GSR (Global State Routing, 1998) etc.

2.2 Reactive (Source-Initiated On-Demand Driven)

These protocols attempt to remove the traditional routing tables and accordingly decrease the requirement for updating these tables to keep track on the network configuration changes. When a source needs to reach a destination, it has to set up a route by route discovery mechanism, manage it by some kind of route maintenance technique until either the route is no longer needed or it becomes inaccessible, and at last tear down it by route deletion mechanism. Some available re-active routing protocols are[7][6] ABR (Associativity Based Routing, 1996),DSR (Dynamic Source Routing, 1996), SSR (Signal Stability Routing, 1997), TORA (Temporally-Ordered Routing Algorithm, 1997), PAR (Power-Aware Routing,1998), LAR (Location AidedRouting, 1998), AODV (ad hoc On-Demand Distance Vector Routing, 1999) and CBR (Cluster Based Routing, 1999). In pro-active routing protocols, paths are always existed (without regarding of requirement), with the signalling traffic and power consumption. On the other side, being more effective at power and signalling consumption, re-active protocols suffer longer delay while route detection. Both classes of routing protocols have been enhancing to be more secure, scalable and to provide support to higher QoS. There are different types of reactive routing protocols: AODV, DSR and TORA.

2.3 Hybrid Protocols:

Hybrid routing protocols integrates a group of nodes into zones in the network configuration. Then, the network is dividedinto zones and proactive mechanism is utilized within every zone to manage routing information. To route packets among various zones, the reactive mechanismis utilized. Accordingly, in hybrid mechanisms, a route to a destination node that is in the same zone is set up without delay, while a route discovery and a route maintenance mechanism isneeded for destination nodes that are in other zones. The zone-based hierarchical link state (ZHLS)routing protocol and zone routing protocol (ZRP)offer a compromise on scalability problem related tothe frequency of end-to-end link, the total no. Ofnodes, and the frequency of configuration change. Moreover, these protocols can offer a better trade-offamong communication delay and overhead, but this trade-off is introduced to the dynamics of a zone andthe size of a zone. Therefore, the hybrid method is asuitable candidate for routing in a huge network

3. JAMMING ATTACK

The jammer is an entity with the aim of attempting to involve in the sending and receiving of data within the wireless communications of network. For blocking the legal traffic of the wireless channel, the jammer continuously emits RF signals. The jamming attacks have common properties that involve the usage of MAC protocols for their interactions [8]. A ratio of the number of packets sent out by any justifiable traffic source to the number of packets to be sent by the MAC layer is taken. This mode of attack has multiple sources instead of just one. These sources send the rough packets to the transmission channels and to the jammed channels as well. This results in packet loss which further decreases the efficiency and reliability

of the system. The problems such as the unavailability of free channel, delay in transmission and new packet drops due to the absence of buffer space are seen.

Physical Jamming (Physical Layer)

Another simple however, disruptive form of DoS attack is the Physical or Radio jamming found in the wireless networks. The reasons behind such attacks are the continuous emission of radio signals or the sending of random bits to other channels. The monopolizing of the wireless medium can be done for causing such attacks by the jammers which can result in denying a complete access to the channel. The channel is to be made idle and the carrier sensing time required is usually large. The nodes enter into a large exponential back-off period, so these results in affecting the adverse propagating affect.

Virtual Jamming (MAC Layer)

The virtual carrier sensing is utilized in IEEE 802.11 for checking the availability of the wireless medium. The attacks on RTS/CTS frames or the DATA frames can be used for introducing jamming at the MAC layer. The MAC layer provides a benefit of providing the adversary node to consume less power while it targets these attacks. The consumed power is less as compared to the physical radio jamming. In this paper, the DoS attacks made at the MAC layer are discussed. These attacks result in collision of RTS/CTS control frames or DATA frames.

- Constant Jammer: A constant jammer is the signal alternator that does not obey any MAC protocol and it continuously released radio signal that represents random bits.
- Deceptive Jammer: They dispatch semi-valid packets. This means that the payload is bootless but the packet header is sustainable.
- Random Jammer: Substitutes between sleeping and jamming the channel. In the first modus the jammer jams for a casual period of time (it can behave like a constant jammer or as a deceptive jammer), and in the second modus (the sleeping mode) the jammer spins its transmitters off for a different random period of time [9]. The energy efficiency is regulating as the ratio of the length of the jamming period upon the length of the sleeping period.
- Reactive Jammer: A reactive jammer attempts not to misspend resources by only jamming when it recognizes that somebody is transmitting. Its object is not the sender but the receiver, taxing to input as much noise as possible in the packet to improve as many bits as possible given that only a small amount of power is required to modify sufficient bits so that when a checksum is execute over that packet at the receiver it will be categorized as not valid and therefore discarded [9].

Jamming aims at fill up the communication channel with pointless signals, due to which verified or permissible user cannot use it. Jamming slows down the request and response of messages at the destination. It is very difficult to prevent and find out the jamming attacks but still some detection algorithms are blind to prevent the prospects of jamming attack. Another motive of Jammers is to conceal themselves from the detection algorithms so that they can begin with jamming of some particular region [10].

4. DETECTION AND PREVENSION METHODS

4.1 Jamming Model

When messages start getting corrupted, this model splits the entire network nodes into three groups. These groups are basically named as Jammed nodes, Boundary nodes and Unchanged nodes. Jammed nodes is located inside the jammed part of network and ultimately it is not able to receive packets from any of its neighbors. Boundary nodes are those nodes which are located to the edge of jammed region, is not jammed but part of its neighbors are jammed. Unchanged nodes are those nodes which are located outside the jammed region and it don't get changed or affect from jamming.

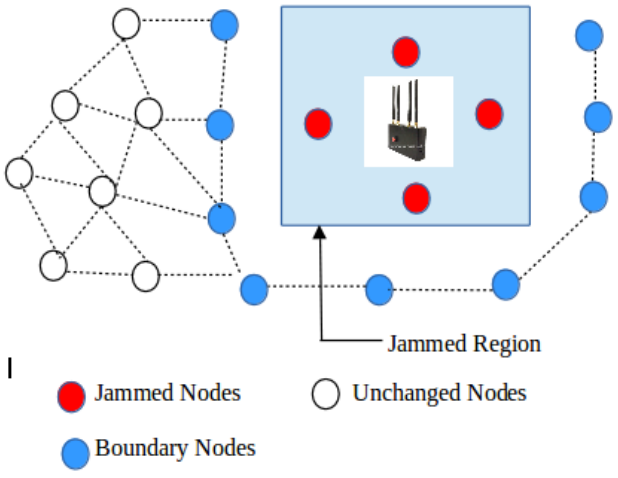

Fig.3 Graphical View of Jamming Module

4.2 Protocols for localizing Jammer:

4.2.1 Centroid Localization (CL)

Centroid based scheme [11][12] is useful for localizing the jammer's position. The main advantage is that it can conduct the estimation without working together with target nodes. First CL gathers the information related to the position of all neighboring nodes which are positioned inside the transmission range of target node. In this model, the neighboring nodes of jammer are called "Jammed Nodes". Thus to determine the jammer's position, CL fetch all co-ordinates of jammed nodes and averages it over their coordinates.

4.2.2 Weighted Centroid Localization (WCL)

WCL[12] is a further step of CL adopted to improve the results by calculating better estimation. In this method, we assume the position of jammer by evaluating their weighted average. This algorithm uses a metric called "Weight" which is the distance between jammer and jammed nodes. Since we don't know how much transmission power is needed and thus it is difficult to find the distance between jammer and jammed nodes. The practicable way to obtain the distance is to compute the RSS (Received Signal Strength) of the incoming signal.

4.3 Jamming Prevention Technique:

4.3.1 Virtual Force Iterative Localization (VFIL):

[7][12][13] VFIL came into picture for achieving better precision than WCL and free from RSS readings. To represent this algorithm, two virtual forces are defined i.e. F-pull initiate by jammed nodes outside the jammed region and F-push initiate by boundary nodes which are placed inside the jammed part. Assume,

(X1, Y1) – estimated place of jammer's
(Xm,Ym) – place of jammed node
(Xj, Yj) – site of boundary node

$$\text{f-pull} = \frac{Xm - X1}{\sqrt{((Xm - X1)^2 + (Ym - Y1)^2)}}, \frac{Ym - Y1}{\sqrt{((Xm - X1)^2 + (Ym - Y1)^2)}}$$

$$\text{f-push} = \frac{X1 - Xj}{\sqrt{((X1 - Xj)^2 + (Y1 - Yj)^2)}}, \frac{Y1 - Yj}{\sqrt{((X1 - Xj)^2 + (Y1 - Yj)^2)}}$$

$$\text{f-joint} = \frac{\sum meJ\ f-pull + \sum jeb\ f-push}{|\sum meJ\ f-pull + \sum jeb\ f-push|}$$

Algorithm**:** [12,13]

Step 0: Detect the jamming attacker

Step 1: Estimate the position of the jammer. Initial estimation is obtained by computing the Centroid of all jammed nodes.

Step 2: Derive the estimated jammed part, which is circle cantered with the radius same as jammed region.

Step 3: Derive F-pull and F-push using above methods, and form the joint force i.e F-joint.

Step 4: Set an adjustable moving step, and move the estimated jammer's position along the direction of F-joint to a new estimate position.

[ii] Honeypots:

[14] Honeypots is a security mechanism employedfor the prevention of jamming attack. In this technique, honeypot are specific nodes which is used to divert the focus of attacker present in the network. The primary function of honeypot is to gain attention of attacker by confining them in a way that attacker will try to attack on honeypot node by thinking that it is dominant area of network. Simultaneously, honeypot will accumulate all the data of attacker like his strategy and purpose. Honeypots are the efficient way for handling jamming attack in wireless infrastructure network.

Algorithm: [14]

Step 1: Scan the current channels to detect the presence of jammer.

Step 2: Ifhoneynode detects the attack

- It immediately informs the base station.
- It continues to communicate with jammer to waste time.
- The base station informs the associated mobile nodes to change the channel of operation.
- The mobile node gets the next channel using pseudo random sequence.

Step 3: If base station detects the attack

- Inform the honeynode about attack.
- Send information to associated nodes.
- If the nodes send response to the base station, then the base station issues a frequency.

- If any of node don't response, the base station broadcast frequency change command and change frequency of operation.

Step 4: If mobile nodes detects the attack

- Wait to receive information from base station.
- If information not received within the time limit, choose the next channel using pseudo random sequence.

5. CONCLUSION

By studying a lot on jamming attack, we are summarizing various approaches and discussed the severe effect of jamming attack in the wireless network.As jamming is a very severe attack to the normal operation of wireless networks, currently much research has been performed to deal with it. All mechanisms are good from their perspective but not best from all points. Mechanisms explained in this paper that can offer information about security functions and a total visual check, which might be appropriate in some applications. But, there is also requirement to model a specific scenario to visualizethe impact of with and without Jamming attack for the improved routing protocol.

6. REFERENCES

[1] Nital Mistry, Devesh C. Jinwala and MukeshZaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[2] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[3] Dimpy Grover, Sunil Saini, "A Survey on Unicast Routing Protocols in Mobile Ad-Hoc Networks" Volume 5, pp. 697-702, May- 2015.

[4] Parul Gupta, "A Litrature Survey of MANET ", in International Research Journal of Engineering and Technology, Volume 03, Issue 02, Feb-2016.

[5] Viren Mahajan, MaitreyaNatu, and AdarshpalSethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[6] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[7] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[8] P. Yi, "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.

[9] Cicho J., Kapelko R., Lemiesz J., and Zawada M., "On Alarm Protocol in Wireless Sensor Networks", IEEE, 2010.

[10] S. D. Babar, N. R. Prasad, R. Prasad "Game Theoretic Modelling of WSN Jamming Attack and Detection Mechanism" Published in Wireless Personal Multimedia Communications (WPMC), 2013.

[11] K Grover, "Jamming in Wireless Networks: A Survey", in Int. J. Ad Hoc and Ubiquitous Computing, Vol. x, No. x, xxxx, 2014

[12] Hongbo Liu, Wenyuan Xu, Yingying Chen, Zhenhua Liu, "Localizing Jammers in Wireless Networks", in IEEE, 2009

[13] Hongbo Liu, Zhenhua Liu, Yingying Chen, Wenyuan Xu, "Determining the position of a jammer using a virtual-force iterative approach", in Springer, 23 October 2010

[14] SudipMisra, Sanjay K. Dhurandher, AvanishRayankula, Deepansh Agrawal, "Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks", in ELSEVEIR, 12 May 2009