International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

A Key Distribution and Monitoring Technique to Detect and Isolate Selective Packet Drop Attack in Ad-hoc Network

Jaspreet Kaur[1], Satish Arora[2]
Computer and Science Engineering, Punjab Technical University
Jalandhar, Punjab, India
[1]preetkhera19@gmail.com [2]arora3683@gmail.com

Abstract—
Wireless Networking is getting extremely dominant now a day as the user need wireless connectivity irrespective of their geographical location. Ad-hoc Network is decentralized, self-organizing and autonomous wireless network in which nodes can join or leave the network whenever they require. The term Ad-hoc means no fixed infrastructure i.e. Dynamic Topology. Aside from these features, Ad-hoc Networks endures from many security issues i.e. active and passive attacks. To develop a mechanism that provides firm security and perceives the malicious node activity in the network. Allowing a secure communication between source and destination is one of major problem in ad-hoc network. This paper describes Key Distribution and Monitoring (KDAM) technique used to detect and isolate malicious node on selective path in AODV routing protocol and secure the channel. The technique provides enhancement over the previously defined methods in terms of delay, packet loss and throughput. The simulation is acted on Network Simulator-2.

Keywords—Wireless Ad hoc Networks; Dynamic Topology; Attacks; Selective Packet Drop Attack

1. INTRODUCTION

To exchange information, a number of devices are joined to together to form network between them. Networking is applied to broadcast information and data communication. Wireless Networking is a technology in which two or more computers referred to as nodes communicates with each other using wireless links. Wireless network can be basically either infrastructure based network or infrastructure less network. The infrastructure networks use fixed base station, which are responsible for coordinating communication between the mobile nodes. The ad-hoc network comes under the category of infrastructure less networks. Ad-hoc Network is gathering of many devices fitted with wireless communication and network capabilities. [7]Ad-hoc Network is decentralized with no pre-subsisting infrastructure, for example a router in wired networks and access focuses in wireless networks on which it is depended. In routing so as to direct every node shares information for different nodes in specially Ad-hoc network the determination of which nodes forward information is made strongly on the substrate of network availability. Ad-hoc Networks are a nascent standard of wireless communication for mobile hosts. Nodes within each other radio range communicate directly by means of wireless connections while these which are far separated depend on different nodes to relay messages. Wireless networks make usage of radio waves or microwaves in order to set up communication between the conveniences. Every node taking an interest in the network behaves both as a host and a router and hence willing to forward packets for other nodes. For this reasons a routing protocol is required.

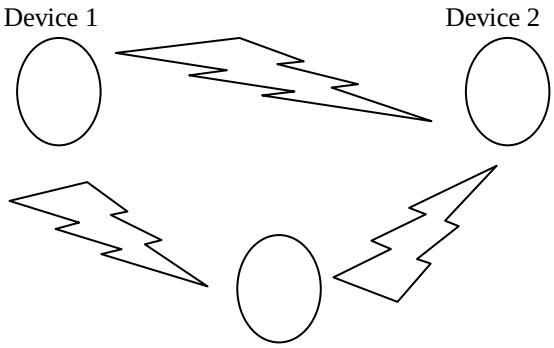

Fig.1 Ad-hoc Network

Wireless Ad-hoc Network is a self-arranging, self-configuring and quickly deployable network in which neither a wired backbone nor a centralized control exists. The nodes are frequently energy constrained. The main characteristics of wireless Ad-hoc networks are -: Dynamic Topology, self-organization, multi-hopping, energy conservation, scalability. Ad-hoc Routing Protocols can be categorized as either Proactive or Reactive. Ad-hoc Networks are threatened to security attacks. Attack is the mechanism which disrupts the normal behavior of the network. There are varieties of attacks possible in Ad-hoc networks. These are discussed below:

A. Passive Attack

A passive attack gets information exchanged in the network without disturbing the operations. The passive attacks are hard to detect as the operations are not influenced. This attack does not disrupt the normal operations of the network. The operations supposed to be achieved by a malicious node which is ignored and attempt to recover significant information by listening to the channel. Snooping and Eavesdropping are examples of passive attacks [3].

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

B. Active Attack

An active attack is that attack in which any data or information is embedded into the network so that data and operation may be harmed. The attacker attempts to alter the data being exchanged within the network. The active attacks disrupt the normal functioning of the network. It includes modification, fabrication and disruption of information which influence the operation of the network. Examples of active attack are impersonation and spoofing [3].

2. LITRATURE REVIEW

Recently Wireless Networks are getting more and more popular. **El-Haleem et al. (2011)** proposes methodology to isolate packet dropping attack by using two disjoint routes protocol in MANET. In this technique two node disjoint routes are selected based in their trust value and use to routes from source to destination. They use DLL-ACK (acknowledgement) and end-to-end Tcp-Ack to identify and examining the behavior of routing path, node. If any malicious node find in the path then path search engine tool get run and identify the malicious node and prevent it [8]. **H-M Sun et al.(2012)** propose an acknowledgment-based technique, called NACK, to detect and mitigate the dropping attacks. Moreover, NACK can resist the collusion attack by using the timestamp mechanism. Although NACK can resist successfully collusion attack, it only considers the case of two consecutive nodes. For our future work, we will enhance the ability about resisting more types of collusion attacks. Compared with other approaches such as the overhearing technique, the NACK scheme has better performance. Our simulation results show that the NACK scheme maintains up to 80% packet delivery ratio in every attack even when the adversary ratio is 40% [10]. **Sharmila et al. (2012)** discussed about the defensive mechanisms based on cumulative acknowledgement and energy based is proposed to detect selective forward attack in mobile wireless sensor networks. The scheme is evaluated in terms of packet delivery ratio and throughput. The malicious node is detected based on the acknowledgement and energy level of the node. The energy consumption of the detection scheme is less when compared with existing detection schemes. From the simulations, byte overhead is 0.39 percentages and detection accuracy is 80% are observed and thus increasing the network throughput. These results show that the packets can be forwarded without any selective packet drop by minimizing the malicious nodes in the network. The further enhancement of the proposed scheme is to improve the success rate to 100% with various mobility and receiver sensitivity of the node [11]. **Aaseri et al. (2013)** discusses Trust Value Algorithm the black hole node can be detected based on the trust values which will result into the low false positive rates. So, Our Approach solves the problem of Packet drop attack with 92% of the success which is far better than the earlier prevention technique to packet drop attack. We used UDP connection to calculate the packets at sending and receiving nodes. If we had used the TCP connection among nodes, the sending node would be the end of the connection, since ACK packets do not arrive at the sending node. The discovery the black hole node with connection oriented protocols could be another future work [16]. **Chuachan et al. (2013)** describes new methodology how to detect and prevent selective packet drop attack. In this paper they discuss 4 previous methods to protect against 1.reputation based 2. Acknowledgement based 3. IDS based 4. Trusted based. The new proposed schema called challenge and response schema. It contain 2 phase I) Key distribution phase II) Challenge ad response phase. The message is encrypted using the public key and routed in two-hop neighbor, take ratio of local one compare it with neighbor node. The malicious node can be detected by setting threshold value to cache and at the end this value to the neighbor's value. To simulate this result they use Common Open Research Emulator (CORE) [18]. **Edemacu et al. (2014)** Wireless ad hoc networks have gained lots of attention due to their ease and low cost of deployment. This has made ad hoc networks of great importance in numerous military and civilian applications. But, the lack of centralized management of these networks makes them vulnerable to a number of security attacks. One of the attacks is packet drop attack, where a compromised node drops packets maliciously. Several techniques have been proposed to detect the packet drop attack in wireless ad hoc networks. Therefore, in this paper we review some of the packet drop attack detection techniques and comparatively analyze them basing on; their ability to detect the attack under different attack strategies (partial and or cooperate attacks), environments and the computational and communication overheads caused in the process of detection [23].

3. SELECTIVE FORWARDING ATTACK

Selective forwarding attack is a sort of denial of service attack where a malicious node draws packets and drops them specifically without sending to the destination. Packet dropping attack is found in the forward stage. So it is extremely composite and hard to isolate. Selective forward attacks may ruin some discriminating applications. In this attack, basically malicious node goes about as normal nodes yet specifically drop sensible packets, for example packet describing the development of the disagreeing forces. Such Selective dropping is very firm to recognize. Counter measures to specific forwarding attacks cannot understand malicious node or include time synchronization. Then again, when malicious node is show on a route by which packets are forwarded, attackers can introduce selective forwarding attacks by merely dropping packets [11].

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

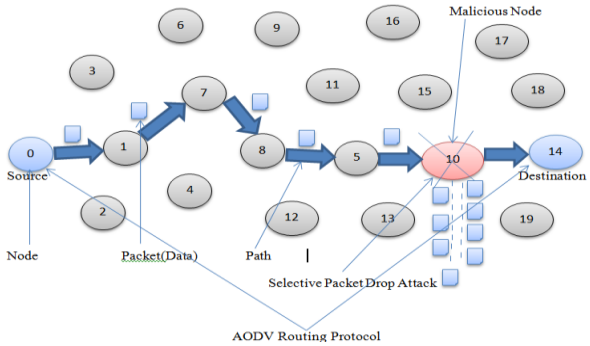

Fig.2 selective Packet Drop Attack

Selective forwarding attacks can root genuine on numerous applications. These attacks have few nodes which drop some or all packets. Attacker can start the selective forwarding attack and stroke the allotment of packets for which it require to store set while forward the rest. This attack is exceptionally hard to distinguish, since packet drops in networks potentially created by untrusted wireless communication or node failure [11].

4. RESEARCH METHODOLOGY

This section represents the methodology used to detect and isolate selective packet drop attack and establishing the secure path in Ad-hoc network.

Step-1 The network is deployed with the finite number of nodes.

Step-2 Source node send the RREQ packets to their adjacent nodes and then Destination node send RREP packets as a reply to select the optimized path.

Step-3 There is a malicious node at the mid of the selected path which drops the packets selectively and only forward the few packets.

Step-4 To detect and isolate the malicious node from the network, the key distribution and monitor mode techniques are used.

Step-5 Now another path is selected for communication where there is no malicious node.

In this way, malicious node will be detected and isolated from the network and secure route is established between source and destination.

V. SIMULATION RESULTS

With the help of Network Simulation (NS-2) we generated the network with 24 nodes as for the Selective Packet drop attack in formal AODV. A UDP is used to create connection between source and destination. With the help of Constant Bit Rate (CBR) traffic is generated.
The simulation has been taken out in NS-2 tool and the parameters used for the validation are discussed below:

Parameters	Values
Terrain Area	800 m x 800 m
Simulation Time	14 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	1000 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	23
Number of Sources	1
No. of Adversaries	1 to 3

Table 1: NS-2 Simulation Parameters

1. Delay: The delay is used to transmit data from source to destination with respect to time. The delay graph shows that packets are broadcast within the network then number of packets can be dropped at particular time interval which is responsible for delay in the network. The x-axis shows the simulation time and y-axis the no. of packets.

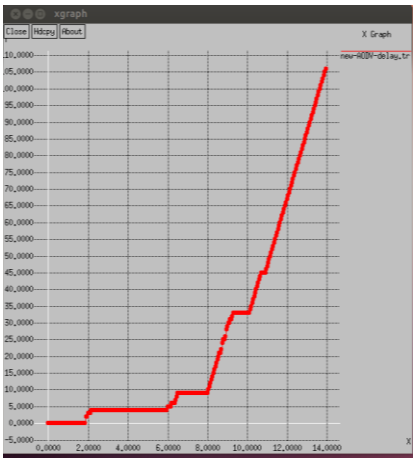

Fig.3 Delay Graph

Fig.3 shows the change in end-to end delay after deployment of the proposed method. It shows that KDAM schema reduce 90% of end-to-end delay while packet is going to transmit from source to destination.

2. Packet Loss: The graph shows the packet loss. The packet loss degrades an overall performance of the network. This graph shows that how many packets can be loss at the particular time interval. The x-axis shows the simulation time and y-axis the no. of packets.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

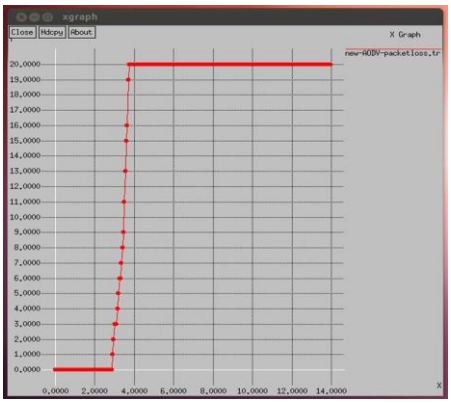

Fig.4 Packet Loss Graph

Fig.4 shows the minimization of packet loss after some time because of secure channel is established between the networks

3. Throughput: The shows the total amount of data a receiver receives from the sender. This graph shows that number of packets can be received by the destination within a particular time interval. The x-axis shows the simulation time and y-axis the no. of packets.

Fig.5 Throughput Graph

Fig.5 represents the throughput after applying proposed method. As delay in the network is minimum because of isolation of malicious node, so throughput of the network is linearly increased after some point of time. From graph we can see that when number of packet increase throughput is gradually increase with time in our proposed schema.

5. CONCLUSION

Ad hoc Network has been vast domain of research work from recent years since its broadly used application in battlefield and business purpose. Because of openness and dynamic topology network is threatened from attacker. The study concentrates on Selective Packet Drop Attack applying AODV protocol. In the past studies, different strategies to detect and isolate Selective Packet Drop Attack which reduce the performance by decreasing latency, throughput and increasing end-to-end delay. In this research work, proposed two network layer schemas Key Distribution and Monitor Mode. The schema detects the malicious node from routing path in the network so whenever new route establish it would free from malicious node then the outcome will be enhanced by throughput increases and minimize delay and packet loss.

ACKNOWLEDGEMENT

I hereby acknowledge that the above referred work is my own research work and I am entirely responsible for any kind of misuse of material. I thank my mentor Er. Satish Arora to guide and encourage me and for putting all his valuable time for me to get the desired output. I also thank my parents and friends who helped me to complete my work with sheer hard work.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P.Agarwal, “Routing Security in Wireless Ad Hoc Network”, IEEE, Volume 40, Number 10, 2002, pp 70-75.

[2] 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, volume 5, Number 3, 2007, pp 338-346.

[3] LathaTamilselvan and V Sankarnarayana, “Prevention of Black Hole Attack in MANET”, Journal of Networks, Volume 3, Number 5, 2008, pp. 13-20.

[4] N.Bhalaji and Dr.A.Shanmugam, “Reliable Routing against Selective Packet Drop Attack in DSR based MANET”, Journal of Software, Vol. 4, Number 6, August 2009, pp. 536-543.

[5] Pradip M. Jawandhiya, Mangesh M. Ghonge “A Survey of Mobile Ad Hoc Network Attacks”, International Journal of Engineering Science and Technology, Vol. 2(9), 2010, pp. 4063-4071.

[6] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, 2011, pp. 107-117.

[7] Priyanka Goyal, Vintra Parmar and Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011, pp. 32-37.

[8] Ahmed M.Abd EL-Haleem and Ihab A. Ali, “TRIDNT: The Trust-Based Routing Protocol with Controlled Degree of Node Selfishness for MANET”, IJNSA, Volume-3, May 2011, pp.189-203.

[9] Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar,” End to End Delay Analysis of Prominent On-demand Routing

Protocols", International Journal of Computer Science and Technology IJCST,Vol. 2, Issue 1, March 2011,pp.42-46.

[10] H.-M. Sun, C.-H. Chen, and Y.-F. Ku, "A novel acknowledgment based approach against collude attacks in MANET," Expert Systems with Applications, vol. 39, July 2012,pp.7968-7975.

[11] S. Sharmila and G. Umamaheswari, "Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012.

[12] A.Baayer, N.Enneya and M.Elkoutbi, "Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETS", Journal of Information Security (JIS), Vol.3, 2012, pp. 224-230.

[13] (2012, 17 May). The Network Simulator - ns-2. Available: http://www.isi.edu/nsnam/ns/.

[14] G.Dini and A. Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," Ad Hoc Networks, Vol.10, 15 March 2012, pp. 1167-1178.

[15] Harjeet Kaur, Varsha Sahni, Dr. Manju Bala," A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, pp.498-500.

[16] Rajendra Aaseri, Pankaj Choudhary, Nirmal Roberts," Trust Value Algorithm: A Secure Approach against Packet Drop Attack in Wireless AD-HOC Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013,pp.99-111.

[17] S.Feslinanish Mon, Raj Kumar Shah, L.Rajaji, "A Progression Based Method for the Detection of Black and Gray Hole Attacks in MANET", IJCNWMC, Volume 3, Issue 3, August 2013, pp. 33-40.

[18] Thongchi Chuachan and Somnuk Puangpronpitag, "A Novel Challenge & Response Scheme against Selective Forwarding Attacks in MANET", IEEE, 2013, pp. 173-177.

[19]Suneth Namal, Konstantinos Georgantas and Andrei Gurtov, "Lightweight authentication and key management on 802.11 with eliptic curve cryptography", IEEE Wireless communication and Networking conference (WCNC), 2013,vol. 48, no. 5, pp.1830-1835.

[20] M.Mohanapriya, Ilango Krishnamurti, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers and Electrical Engineering, Vol.4, February 2013,pp 530-538.

[21] K.Sangeetha, "Secure Data Transmission in MANETS Using AODV", IJCCER, Volume-2, Issue 1, January 2014, pp. 17-22.

[22] Apurva Jain and Anshul Shrotriya," Prevention of Black Hole Attack on MANET Using Trust Based Algorithm", International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014,pp.408-413.

[23] Kennedy Edemacu , Martin Euku and Richard Ssekibuule," Packet Drop Attack Detection Techniques in Wireless Ad-hoc Networks: A Review", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.5, September 2014,pp.75-86.