TRUSTBASED PREVENTION MECHANISM FOR SELECTIVE JAMMING ATTACK

Lalit Gehlod,Mala Dutta,Nikita Mulatkar
Institute of Engineering & Technology, D.A.V.V.
Indore, Madhyapradesh, India

***Abstract*— Security is a basic requirement in mobile adhoc network to provide a secure communication between the mobile nodes. Mobile adhoc network(MANET) is a kind of wireless network which do not rely on any predefined infrastructure. Due to the open nature of medium mobile adhoc network is vulnerable to various attack. In this paper, we focus on selective jamming attack in which the adversary targets the message of high importance such as routing message. To mitigate these attacks some cryptographic primitives are used but this method introduce higher computation overhead. To reduce such overhead we design a new mechanism which can detect the attacker or jammer node with lower computation and communication overhead. In this paper, we proposed a Enhance Trusted Adhoc On Demand Distance Vector Routing protocol (ETAODV), which is a modification of well known adhoc on demand distance vector routing protocol (AODV). Proposed Enhance rust based adhoc on demand distance vector routing protocol(ETAODV) protect the network by identifying the malicious behavior of node with the help of trust value. The communication among the nodes depends on the trust value of node with its neighbor. The simulation result in NS2.35 exhibit that our proposed protocol not only prevent the network from malicious node but also enhance the overall performance in terms of Throughput and Packet Delivery Ratio without applying any cryptographic method.**

Keywords— selective jamming attack, ETAODV, MANET

INTRODUCTION

A wireless network is a network which utilize wireless media such as radio frequency technology to transmit and get information over the air, limiting the requirement for wired connection. A mobile adhoc network (MANET) is collection of mobile nodes in which the nodes dynamically located in such a way that the intermediate connection between them change continuously therefore the network confront different security issues such as anyone with a transceiver can infuse spurious messages or jam legitimate ones. Jamming is a one of them attack which interrupt the standard functioning of network, while message infusion can be anticipated by utilizing some cryptographic primitives, but jamming attacks are significantly harder to counter. An adversary can use different attack strategies to jam wireless communication. The jammer can be classify as follows [10-11]:

i. Constant jammer: The constant jammer is a type of jammer which consistently emits a radio signal and implemented by using a waveform generator which constantly send a radio signal or a ordinary wireless device that continually send the random bits to the channel.

ii. Deceptive Jammer: Rather than sanding random bits, this type of jammer continually infuses regular packets to the channel without any gap between consequent packet transmission.

iii. Random Jammer: Instead of constantly sending out a radio signal , this jammer alternate between two modes sleeping and jamming. During jamming mode, it behave like either a deceptive jammer or a constant jammer. After a jamming , it enters in sleeping mode and turns off its radio.

iv. Reactive Jammer: the reactive jammer sending out a radio signal when it senses any activity on the channel.

In simplest form of jamming attack the adversary interfere with the message by transmitting continues jamming signal [7] or several short pulses[8].Typically jamming attack have been analyzed under in external model , in which the adversary is a not a part of network. In this type of attack the adversary continues emit the high power interference signal[9]. However adopting “always-on” strategy has numerous disadvantages. First , the adversary has to consume lot of energy to jam frequency band. Second, the presence of high interference level makes this type of attacks easy to detect.

Some conventional anti jamming technique such as spread spectrum techniques are used to protect the wireless transmission under the external model. Spread spectrum technique give bit level security by spreading bits according to a secret pseudo-noise(PN) code, which is known to the parties which want to communicate with each other. These strategies can provide security under the external threat model.

In this paper ,we address the problem of selective jamming attack under an internal threat model, in which the adversary is a part of network and selectively target the message of high importance such as routing message(RREQ and RREP).To mitigate these attack we proposed a new mechanism by modifying the demand distance vector routing protocol (AODV) and this protocol is known as N-Trust based adhoc on demand distance vector routing protocol(NTAODV). The

proposed mechanism protect the network by identifying the malicious node without apply any cryptographic primitives with the help of trust value.

RELATED WORK

In [1] prano et al. proposed a work in which they use some cryptographic primitives such as strong hiding commitment scheme ,hiding based on cryptography puzzle and All or nothing methods. but this method introduce higher computation overhead and also decrease the effective throughput of the system as compare to no hiding method.

In [6] Brown et al. consider the problem in which an attacker disturbing an encrypted wireless adhoc network through jamming. To prevent the selectivity, entire packet and payload are encrypted.

In [3],Lazos et al. address the problem of control channel jamming attack in multichannel adhoc network and provide a randomized frequency hopping algorithm to protect the control channel from inside jammer.

In [4] ,Law et al. proposed selective jamming strategies for well-known sensor network MAC protocol. They develop jamming attack which work on encrypted packet and are as effective as constant/deceptive/reactive jamming.

In [5], some conventional methods are used for mitigating non selective jamming attack for this purpose they employ some form of spread spectrum communication.

BACKGROUND

AODV is a one of the most popular Reactive Routing Protocol for MANET's. Therefore, routes are determined only when needed. Whenever an AODV router or node receives a request to send a message, it checks its routing table for route existence. Each routing table entry consists of Destination Address, Next Hop Address, Destination SN and Hop Count.

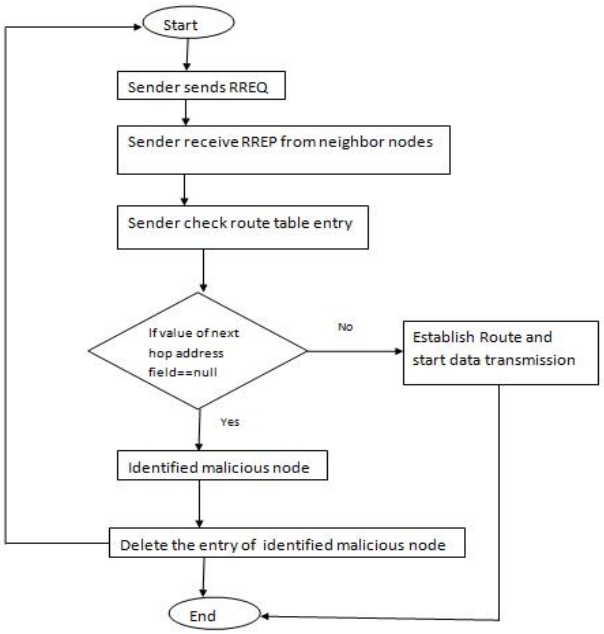
Routing discovery happens when any source node desire to send a packet to some destination and does not have valid route for that destination. It checks routing table to determine if it has a current route to the destination, while it obtain no proper route entry for that destination, this source node create RREQ(Route Request) packet and broadcast to all its neighbor node. Each neighbor who receives this RREQ check in its routing table , if receiving node is not the destination node and does not have a current route to destination , it will setup a reverse path towards the originator of RREQ and rebroadcast the RREQ . AODV uses destination sequence number to guarantee all routes are loop free and contain the recent information about route. Each node contain its own broadcast ID and also a sequence number. The broadcast ID is augmented for each RERQ the node created together with node's IP address, uniquely distinguishes an RREQ. Along with its own broadcast ID and sequence number the source node includes the recent sequence number in the RREQ for the destination node.

Any node can reply to RREQ only if it has a valid route to the destination and whose consequent destination sequence number is greater than or equivalent to that contained in RREQ.

Once an intermediate receives RREQ it generates a RREP(Route Reply) packet. The RREP is unicast to the next hop towards the originator of the RREQ as indicated by the routing entry for that originator. Each intermediate node which receives an RREP packet, it first updates some field of routing table and route reply packet ,then forward it to next hop towards the originator .In this way RREP will ultimately reach the source node , the source node records the route to the destination and begin the transmission of data packets.

PROPOSED WORK AND FLOWCHART OF PROPOSED SOLUTION

The proposed mechanism does not apply any cryptographic primitives on the routing messages instead it protect the network by identifying the malicious behavior of node with the help of trust value. Here we consider the value of next hop address field of a routing table as trust value. In our Proposed solution any node on receiving a RREP packet (which is reply to the route request), first of all Cross check the routing table of next hop in the route to the destination, if the next field (field of next hop in the route) does not have any value or route to the destination then the node sent the RREP is considered as malicious node.



Flow Diagram of ETAODV

The following steps describes the activity of an individual node participating in the communication:

Step 1: Source node sends a RREQ to its neighbor node.

Step 2: Awaits for RREP from its neighbor node

Action By intermediate node/ Destination Node :

1. On receiving the RREQ From source it first makes entry in its routing table.
2. If it is not a destination node nor does it have fresh enough route to the destination node, then it forward the RREQ to its neighbors.
3. If it is the destination node or it has route to the destination node, then it replies to the source node with an RREP.

Step 3: On receiving an RREP from the any node the source node update its routing table.

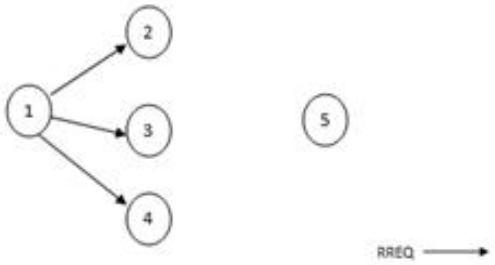
Step 5: Detection of malicious node:

1. After the updation of routing table source node initiate the process of malicious or jammer node detection by cross check the routing table of next hop to the destination.
2. If the value of next field (trust value)==null, then the node is identified as malicious node and source will delete it entry from the its routing table.

Illustration of proposed solution:

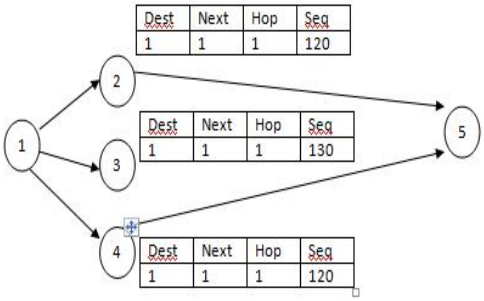
We use the following figure as an example here we assume that node 1 is a sender who want to communicate with node node 5. we also assume that the node 3 is a malicious node between them who interrupt the communication between them by sending a false RREP to source node this makes the source node that it has a route to a destination. Our proposed solution will detect the malicious behavior of the node by using following steps:

Step 1: Node 1 (source node) broadcast RREQ to all it neighbor node (node 2, node 3, node 4).

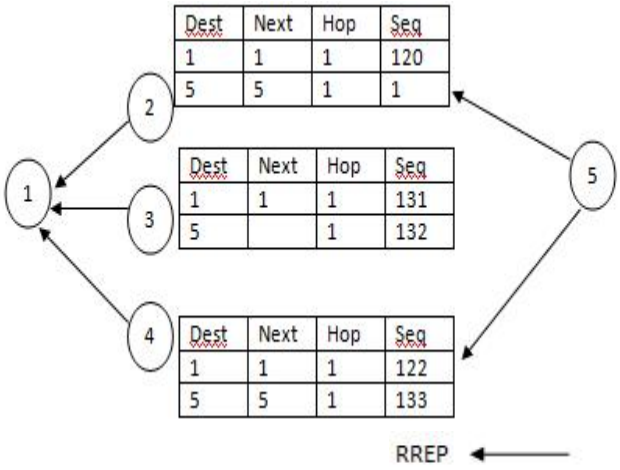


Step 2:

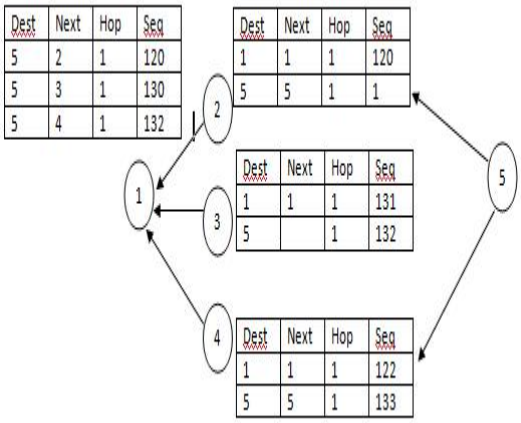
1. On receiving RREQ from source node its neighbor node(node 2, node 3, node 4) first makes entry in its routing table and forward the route RREQ to node 5.



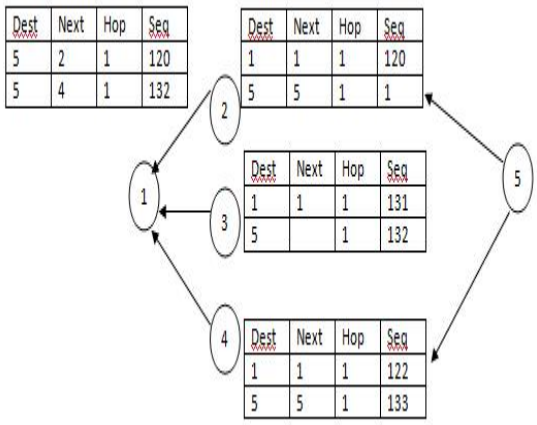
2. Since node 5 is a destination node it unicast the RREP to source node.



Step 3: on receiving RREP from its neighbor node source node updates its routing table.



Step 4: After updation of routing table the node 1 initiate the process of malicious node detection by cross check the routing table of node 2, node 3, node 4 and check the value of next field (trust value). Here the value of next field (trust value) of node 3 == null. in this way node 3 is identified as malicious node and delete its entry from routing table.



SIMULATION RESULT AND ANALYSIS

In this section we create mobile adhoc network in NS 2.35 with different number of nodes (20 nodes, 30 nodes, 40 nodes). The table 5.1 shows different parameters used in simulation by every node.

Table 5. 1 Parameters used in simulation

parameter	value
Simulator	NS 2.35
Network Size	750m*750m
Radio Propagation model	TwoRayGround
Channel Type	WirelessChannel
Routing Protocol	ETAODV,AODV
Traffic Area	CBR
MAC Type	802.11

The implementation is done in following three sections:
Section 1: In this section we configured a mobile adhoc network for different number of nodes. Nodes use aodv protocol for route discovery.
Section 2: In this section we introduced a jammer or attacker node in the network.
Section 3: In this scenario, we applied proposed enhance trusted adhoc on demand distance vector routing protocol (ETAODV) on network.
All sections are implemented for 20 30 and 40 nodes in NS 2.35 simulator. The nodes are considered to be mobile. In order to evaluate the performance of proposed Enhance trusted adhoc on demand routing protocol (ETAODV) we used three performance matrics: Throughput, Packet Delivery Ratio, End to End delay. A brief description of performance metrics is gives as follows:

Performance Parameter
In order to evaluate the performance of proposed N trust based adhoc on demand routing protocol (NTAODV) we used following matrics :

i. Packet Delivery Ratio (PDR): The proportion of the number of data packet received by the receivers to the number of packet supposed to be received. It is given by

   PDR= received packets/generated packets * 100

ii. Average End to End Delay: End To End delay refers to time taken for a packet to be transmitted over a network from source to destination.

iii. Throughput: Throughput is a measure of how many units of information a system can process in a given amount of time. Typically, throughputs are measured in kbps, Mbps and Gbps.It is given by

   Throughput= received_data*8/Data Transmission Time

Fig.5.1 shows that when we applied the proposed enhance trust based adhoc on demand routing protocol (ETAODV) on a network it detects the malicious node in the network and also provide better throughput then existing AODV protocol with in increase in number of nodes.

Figure5.2 shows the packet delivery ratio between proposed enhance trusted adhoc on demand routing protocol (ETAODV) and AODV protocol. Packet delivery ratio (PDR) is a ratio of packets that are effectively transmitted to the destination node compared to the packet that have been send by source node. The proposed enhance trusted adhoc on demand routing protocol (ETAODV) transmit more number of packets as compared to AODV protocol.

Figure5.3 shows end to end delay between proposed enhance trusted adhoc on demand routing protocol (ETAODV) and AODV protocol. The proposed protocol has more end to end delay with increase in number of nodes.

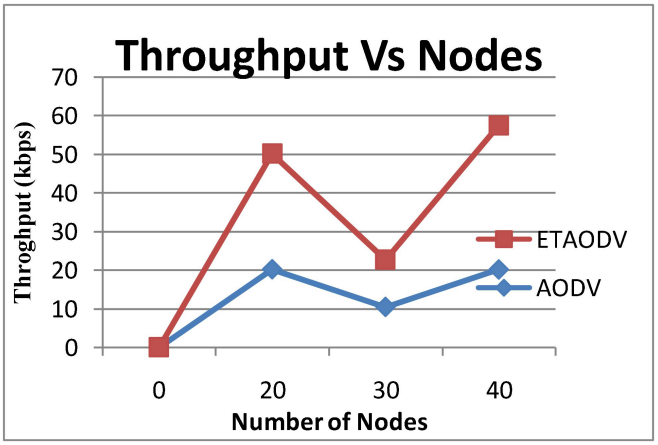


Figure 5.1 Throughput Vs Nodes

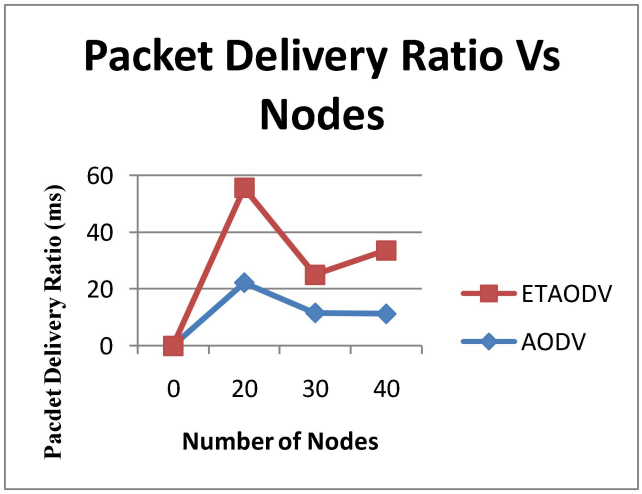


Figure 5.2 Packet Delivery Ratio Vs Nodes

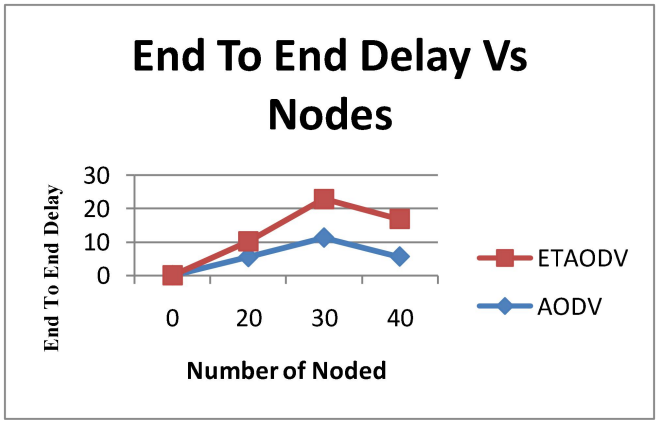


Figure 5.3 End To End Delay Vs Node

CONCLUSION

In this work we focused on selective jamming attack in which the jammer node selectively target on a routing massages in a mobile adhoc network(MANET). Mobile adhoc network is a group of mobile nodes that can communicate with each other without any infrastructure, due to the lack of infrastructure this network is open to various attack. The jamming attack is one of them attack which interrupt the functioning of the networking.To mitigate this attack we proposed a novel mechanism which is called N-Trust based adhoc on demand distance vector routing protocol(NTAODV) . This proposed trust based routing protocol detect the malicious behavior of attacker or jammer node without applying any cryptographic primitives with lower computation overhead.

REFERENCES

1. A. Proano and L. Lazos, "Packet-Hiding Methods for Preventing Selective Jamming Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 101–114, 2012.
2. X. Li, M. Lyu, and J. Liu, "A trust model based routing protocol for secure ad hoe networks," *IEEE Aerospace Conference Proceedings,2004*
3. L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-Channel jamming Attack in Multi-channel Adhoc Networks," *Proceedings on ACM conference on wireless security*, pp. 169–180, 2009.
4. Y.W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. "Energy-efficient link-layer jamming attacks against WSN MAC protocols," *ACM Transactions on Sensors Networks* , pp. 1–38, Apr. 2009.
5. Y. Desmedt, "Broadcast anti jamming system", *Computer network*. Februry, 2004.
6. T. X Brown, J. E. James, A. Sethi, "Jamming and sensing of encrypted wireless ad hoc networks," *In Proceedings of MobiHoc*, pp. 120–130, 2006.
7. M. K. Simon, *Spread spectrum communications handbook*. New York: McGraw-Hill, 2002. Nubir and G.lin, "Low Power Dos Attack In Data Wireless Lans And Countmeasure", *Mobile Computing And Communication Review*, 2003
8. G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, p. 29, Jan. 2003.
9. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing - MobiHoc 05*, 2005.
10. Y. Law et al, "Link-Layer Jamming Attacks on S-Mac", *Proc 2nd Euro workshop*, wireless Sensor Network,2005
11. A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.