DETECTION AND PREVENTION OF MALICIOUS PACKETS DROPPER IN MANET USING DIFFIE-HELMAN PACKETS EXCHANGE APPROACH

Sibomana Fabrice[1], Dr.E.J.Thomson Fredrik[2]

ABSTRACT

Mobile Ad hoc network is one of the wireless networks that is more popular nowadays due to its application suitability. MANET network has a role to play in different fields such as the military. Backup service also is one of the important applications of MANET (tragedy, recovery, quick diagnosis or record handling in the hospital). It is worthy also to mention the vulnerability of MANET. Providing MANET security is not an easy task due to its dynamic nature and lack of central control point. In MANET routing protocols are needed to help discovering routes. AODV protocol is one the popular protocols used in route discovery process while routing packets to the intended destination in MANET, but AODV is also prone to well-known packet dropper attacks. MANET is prone to so many kinds of attacks that undermine network performance. Multiple strategies and mechanisms have been proposed to tackle those attacks in terms of improving network performances and network reliability, but still there is a need of strong better mechanism in MANET in order to provide an even better defence from attacks. Therefore, a new mechanism is proposed that tackles all kinds of packet dropper attack. This mechanism uses two packets (source diffie-hellman and destination diffie-hellman packets) to find whether a selected path between source and destination node is malicious. If so then the behavioural analysis approach is used to identify and eliminate the malicious nodes from the path based on their behaviour.

Keyword : MANET, NTT, Malicious node, malicious path, Packet dropper

I. INTRODUCTION

Mobile Ad hoc network is a self-configuring, self-maintaining network of mobile nodes and it is more susceptible to attacks than wired networks due to the fact that it does not possess central administration point and lacks infrastructure. In MANET, node can join or leave the network at any time and each new node has to authenticate itself to other nodes. Mobile nodes in MANET communicate with one another through wireless links and routing protocols that are used to discover the route between source and destination. The level of vulnerability is so high in MANET due to the nature of mobile Ad hoc network (lack of infrastructure, dynamic topology, lack of central administration, network scalability etc.). During the transmission process, there is a possibility that the packet can be dropped, delayed, altered or forwarded to the wrong node. Each node in MANET must deliver its credential and identity in order to participate in any transmission process so that authenticity and integrity of communication can be maintained. Unauthorized participation of malicious node attempts to reduce the

[1] Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Tamilnadu, Coimbatore - 21, India

[2] Associate Professor, Department of CS,CA & IT, Karpagam Academy of Higher Education, Tamilnadu, Coimbatore - 21, India

performance of the network or even paralyze the whole network in the worst case. Ad hoc network faces security threats of many kinds. Malicious nodes pretend to behave similarly to the legitimate node and take advantage of the network resources and cause the network to become imbalanced thereby reducing the throughput.

MANET experiences many serious attacks, one of which is classified as packet dropper attacks. This attack drops packets or diverts packets in the case of collaboration attack. Such attacks are black hole, gray hole and worm hole attacks. Gray hole attacks are difficult to detect since they maliciously keep changing their behaviours [1]. Source gray hole attacks are the ones that will drop any packets originating from a particular source node, whereas destination gray hole attacks are the ones that drop the packets that are heading to a particular destination node [1]. Worm hole attacks work in a group where malicious nodes collaborate with one another to perform their attack in MANETs. Malicious node that receives the packet forwards it through another route instead of forwarding it to the intended destination node. Then that packet is diverted in that group of malicious nodes [1]. Black hole attacks are attacks that advertise themselves to have the best path to destination and once they receive the packet they drop them [2]. Thus, in all above cases the network performance will deteriorate greatly. That is why it is very crucial to introduce a stronger mechanism that will detect and eliminate these kinds of attacks. This study proposes a system that will determine whether a path between source and destination node is a malicious and whether in a malicious path there is one or more malicious nodes. The behavioural analysis approach is used to establish trust among nodes in the path.

Section 2 covers briefly previous literature related to the proposed defence mechanism, Section 3 details of the proposed mechanism, Section 4 how the method is implemented, Section 5 the simulation results and Section 6 conclusion.

II. RELATED WORKS

P.N. Karthick and R. Bamalakshmi [4] proposed an approach for detecting and preventing malicious packets dropping attack using an algorithm called Blow Fish Algorithm. This approach helps also in distinguishing whether the packet prop was intentional in the case of link error or unintentional in case of malicious packet dropper attack.

N. K Gupta and pandey [3] have proposed a trust-based routing algorithm considering the honest value of the participating nodes with Ad hoc on-demand distance vector routing (AODV) as the routing protocol. The honest value also known as trust value is used in addition to the hop count. Honest value is incremented during route request (RREQ) phase and decremented during route reply (RREP) phase. Depending on the hop value the best path is arrived as further enhancement. Before forwarding the data, the node evaluates the routing path according to trusted metrics using HAODV (hybrid-AODV).

Krishnaveni Nunna et al. [5] has proposed a new protocol called Secured Ad hoc on Demand Distance Vector (SAODV) that detects and prevents packet dropping attack in MANET. The new protocol can detect malicious nodes by Identifying dropping of routing and data packet. And both packet dropping due to link error and malicious node can be detected by the proposed protocol.

Sujath et al. [9] discuss the use of genetic algorithm with a soft computing technique which implements the

law of selection and evaluation. This method is used in high traffic networks to distinguish between genuine and malicious connections thereby reducing black hole attack.

S. Madhurikkha and R. Sabitha [6] have proposed a mechanism to detect where legitimate routing Information is used to detect and prevent packets proper attack in MANET. The mechanism uses two techniques called Data Routing Information Table (DRI) and Cross Check. Data routing Information table stores two bits (1, 0) one and zero. The node responding to the RREQ from source should send RREP along with a DRI table containing 0 bit stands for TRUE and 0 bit stands for FALSE regarding the entries in the network. Cross Check is used to check the reliability of the node. If the packets have passed through a particular node that node is considered truthful. This mechanism was used before by Jay Dip Sen in 2011 for defending against black hole attack but the author also mentions that the techniques could be used to defend packets dropper attack from MANET.

K. Bradley et al. [10] have come up with "WATCHERS", a behavioural approach on the basis of the principle of packet flow conservation which detects and reacts to routers that drop or misroute packets. Here the number of packets in coming to a node expect the ones destined to it, and the number of packets forwarded by the node except the ones generated by it, and validated periodically by all the neighbours of the suspicious router. Similarly, a mechanism that detects bad routers which group with neighbours and those that alter packets are proposed to be addressed with suitable authentication mechanisms.

Akansha Shrivastava and Ekta Chauhan [7] have proposed an approach called Zone-based Path Routing approach. The proposed system detects and prevents malicious behaviour of nodes in MANET.

V. Balakrishnan and Varadharajan [8] combine the fellowship model with energy level model. Here the nodes have the obligation to follow the fellowship model in order to stay inside the network. The commitment to render network services inside the network is calculated using the energy levels of the participating nodes. It involves the parameters such as proportion of outgoing energy and the initial energy. Depending upon the activeness of the node, using the energy level is directly proportional to the possibility of the node being honest with a threshold. The nodes are isolated from the network if they behave maliciously. However, a large computation of energy levels using complex mathematical computation at every node inside network leads to a huge overhead.

U. Venkanna and Velusamy [11] have proposed a trust management scheme to detect and isolate the compromised nodes. The WATCHDOG strategy is used to observe the behaviour of the suspected nodes. The information about the behaviours of the nodes is fed to the reputation system (RS) updated by reputation table. Roy et al. have proposed a dynamic trust management system (DTMS) that helps to distinguish between legitimate node and malicious node in the network.

Rutuja et al. [1] have introduced an approach that called Secure-BEFORE Routing Strategy that ensures optimal route estimation in computing the trust value and hop counts using Dummy packet inside network at 1-hop level. The dummy packet is sent by source node through intermediate node and once it reaches the destination the destination node sends back the confirmation signal through the same intermediate

genuine node the dummy packet came in. They are genuine because malicious nodes either drop or divert the packets. Once the source node receives the confirmation signal it starts the data transmission process through the genuine node.

Yaser Khamayseh et al. [2] have proposed a trusted scheme that detects and prevents malicious nodes from the network based on node behaviour. The trusted scheme monitors and evaluates the behaviour of all nodes in the network by establishing a threshold value that stands for the trustworthiness of each node. Each node in the network observes the behaviour of its neighbour nodes and then passes this value along with other observations to the nodes in the network. Then the behaviour of neighbouring nodes is used as an indication to identify whether a node malicious or not.

III. PROPOSED SYSTEM DESIGN

Malicious path identifier method that uses two diffie-hellman packets (S diffie-hellman packet and D destination diffie-hellman packet) is used to determine whether the chosen path is a malicious path or valid path. If the path is found to be malicious then behaviour analysis approach is used to identify and isolate various malicious attacks present in the path since malicious path contains one or more malicious nodes. This proposed solution will help to improve the overall performance of the network.

For establishing a communication between source node and destination node, when the source node sends RREQ message, the intermediate nodes that have the route to the intended destination respond with RREP message back to the source node.

Source node will receive RREP messages from different nodes. Then it considers the RREP message that has the shortest route to destination for further process. Source node prepares S diffie-hellman packet by computing its public key which will be sent in the dummy packet. Source node sets a timer and then S diffie-hellman packet is sent through intermediate node towards the destination node and waits for the D diffie-hellman packet (which also contains computed public key from destination) which is received at source node through the same intermediate node that S deffie-hellman packet came in.

S diffie-hellman is received at the destination node only because it goes through genuine nodes. For malicious node either drops or diverts the packets without forwarding them to the intended destination. If the timer set by source node is expired before it receives the D diffie-hellman packet from destination. The source node considers that path to be a malicious path but if the source node receives the response from destination in time that path will be considered as valid path and the data transmission process will take place between source node and destination node with encrypted message.

Two diffie-hellman packet scenario illustration

Two diffie-hellman packets are used to determine whether the chosen path has a packet dropper node or not.

Step1: Source node chooses the path from RREP it has received from different nodes and then prepares its diffie-hellman packet by choosing three numbers namely,

Prime number (P) = 17

Generator (G) = 3

Private number = 10 and then computes its public key

Source public key (s Pk) = 310mod 17 = 8

Step 2: Source node sends its diffie-hellman packet containing (P=17, G=3, SPk=8) after setting the timer and waits for the response from destination node with D diffie-hellman packet. This packet can only reach at destination node through genuine node, for malicious node either drops or diverts the packet instead of forwarding it to the intended destination node.

Step 3: Upon receiving S diffie-hellman packet from source node, destination node chooses its private number and computes its private key.

Private number = 12

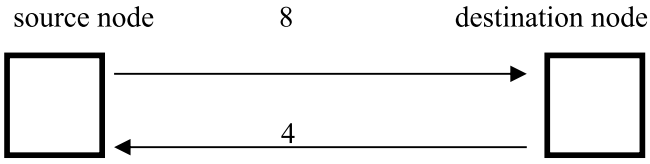
Prime number (P) =17

Generator (G) = 3 and then computes its public key

Destination public key = 312mod 17 = 4

Step 4: Destination node sends its D diffie-hellman packet back to the source node (containing public key = 4) if the packet reaches at the source node. The source node confirms that the path is not malicious, but if the timer expires before the D diffie-hellman packet has reached then the path is considered malicious.

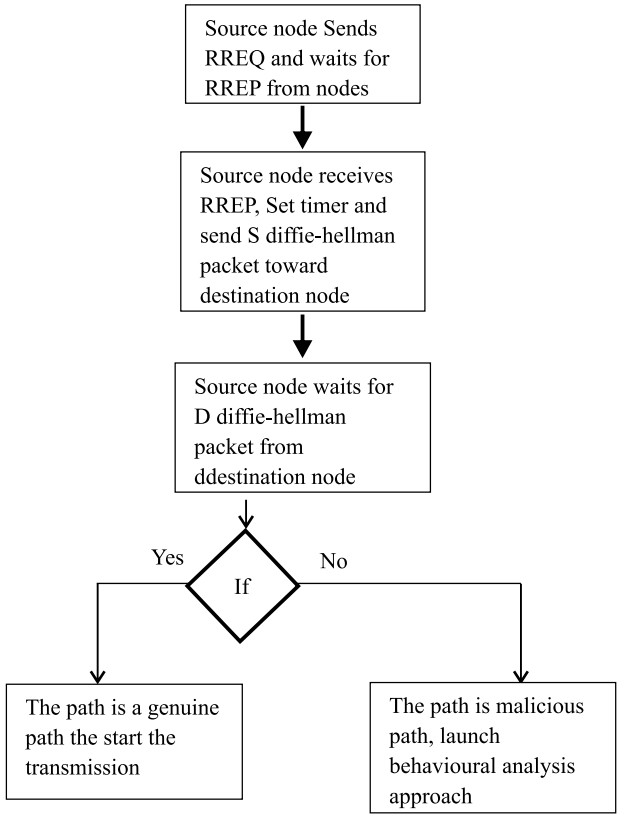
Step 5: If the path is found to be a genuine path, both source and destination nodes calculate the secret keys to use during the transmission process.



Source secret key= 410mod 17=16 Destination secret key=812mod17=16

This secret key (16) will be used to encrypt the messages in the data transmission process.

Flowchart of proposed system



Algorithm 1: Malicious path detection Algorithm

Broadcast RREQ message by Source node and then upon receiving RREP message from neighbour node.

Source node prepares a diffie-helman packet by choosing three random number namely

Prime number (P) = 17

Generator (G) = 3

Private number (p)= 10 and then computes its public key

Source public key (s Pk) = 310mod 17 = 8

Source node sends a prepared diffie-helman packet (P=17, G=3,sPK=8) and then transmission time is noted as (t1)

Destination node upon receiving source diffie-Helman

packet from source node, prepares its own diffie-helman packet by choosing its own three random numbers

Private number = 12

Prime number (P) =17

Generator (G) = 3 and then computes its public key

Destination public key = 312mod 17 = 4

Destination node sends a prepared Destination diffie-helman packet (P=17, G= 3, dPk = 4) back through the same path Source diffie-helman came through and then the reception time is noted as (t2).

RTT is computed using the following equation:

Tsi= t2i - t1i

Find the threshold using the following equation:

Tth = tsi/hopi

The obtained time is marked as threshold RTT Tth for the path (i)

If Tsi < Tth then the path will be considered as malicious path, Mark the path I has the presence of packet droppers attack in it.

Else

The path is considered as a genuine path and encrypted messages are transmitted through the path.

A genuine trusted connection is established between source and destination.

IV. PACKET DROPPER PREVENTION MODEL

In the case of malicious path. Behaviour analysis approach is launched in the path. The main purpose of this approach is to detect and eliminate malicious nodes in the path. The scheme evaluates behaviours of each node in the considered malicious path. Each node in malicious path observers the behaviour of its one-hop neighbouring node and every node has Neighbour Trust Table that records the activities of its neighbour node.

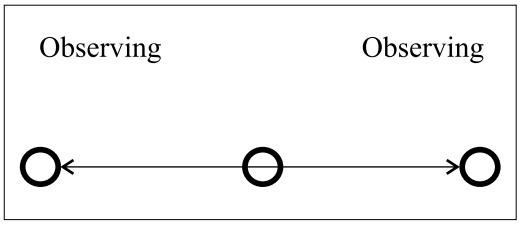


Figure 1: Node D is directly observing the behaviours of its one-hop neighbours F and C and it stores the values of their behaviours in its Neighbour Trust Table.

Neighbour Trust Table

Each node in the path builds a Neighbour Trust Table that keeps track of the information observed directly from each of its one-hop neighbour in the path, in order to calculate the trust value of node. The NTT contains entries only for one hop neighbour nodes. Once the path is found to be malicious path, the behavioural analysis will be launched with the threshold calculated while determining whether the path is malicious. Behavioural analysis uses trustworthiness evaluation formula to identify and isolate packet dropper attack in the path

Trustworthiness evaluation formula

Trustvalue=A1*Mobility+A2*Datareceived+A3*Datasent+?4*Oldtrust

Trustworthiness evaluation formula uses the data stored in NTT where A1, A2, A3 and ?4 represent the tuning constants which are found during simulation. The sum of these constant equal to 1, Datareceived are the data received by the observed node, Datasent is the data sent by the observed node and Oldtrust is the previous trust value of a node.

NTT structure for node D is shown in the table below. D node has entries of node F and C and their behaviour values. Node D calculates trust value for each of its one hop neighbour nodes using the stored value as demonstrated in the formula.

Node	Mobility	Datasent	Datareceived	Oldtrust
F	0.6	0.91	0.35	1.6
C	0.7	0.10	0.57	1.23

Once the path is considered as malicious node, source node lunches behavioural analysis process by sending threshold value through the path, and each node in the path uses trustworthiness evaluation formula to calculate the trust value of its one hop neighbour nodes. The trust value found is compared with the threshold sent by source node. If the trust value of a node is lower than that of that sent by source node then that node will be identified as packet dropper and removed from the network.

V. PERFORMANCE EVALUATION

The proposed approach is simulated using NS2 to evaluate the performance of the proposed system by exchanging the Diffie-hellman packets through the chosen path with RTT during the course of that exchange. It determines whether it is malicious path or genuine one. Table 2 shows the parameter values used to experiment the proposed system.

Parameters	**Value**
Area	900*900
Time	500 s
Protocol	AODV
Nodes	Normal node: 50 Packet dropper nodes: 2
*Min*_RC	3
*Max*_RC	7
*Min*_TV	5
*Max*_TV	10
Transmission Range	250 m
Mobility	Random mobility, 0 – 25 ms
Maximum number of connections	50 nodes or 25 pairs
Type of traffic	CBR
Size of data packet	512 bytes
Maximum speed of packets	25 ms
Pause Time	0 – 20 s

VI. SIMULATION RESULTS AND DISCUSSION

The proposed approach is experimented using a tool called NS2 tool. The first figure shows the network with malicious nodes that have been detected. The second figure shows results of the network under malicious packets dropper attack with the proposed approach to tackle the attacks. Figure 3 shows the result of the network under malicious packets dropper attack without any system in place to defend it.

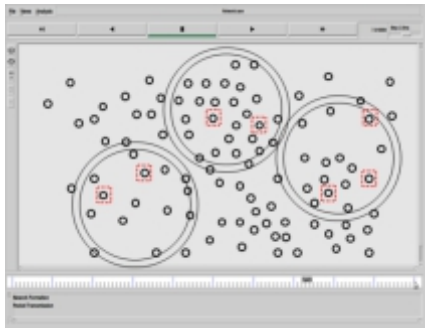


Figure 1: The figure shows dropper attacks detected in the network which needs to be isolated from the network.

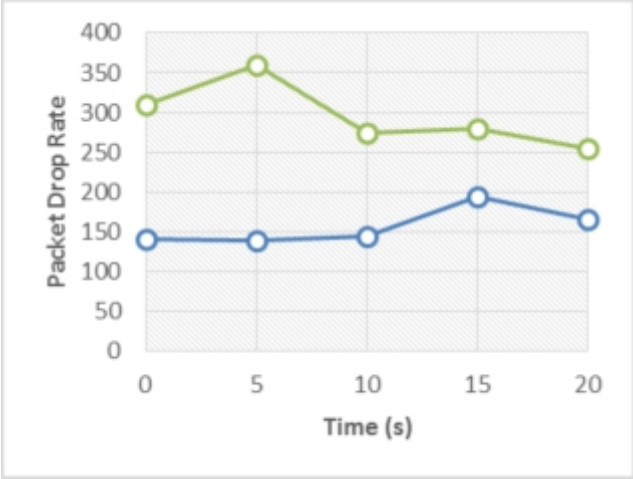


Figure 2: Proposed Network Model
Time(s) vs Number of Packets Dropped

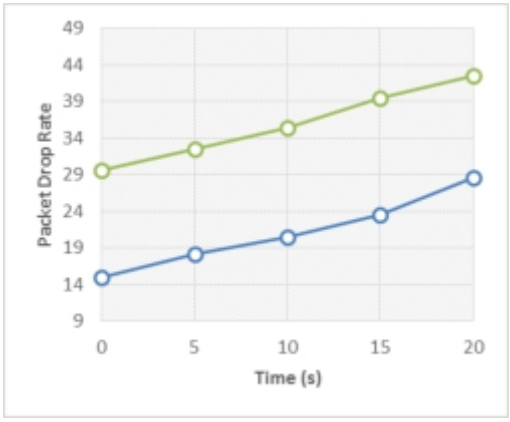


Figure 3: Malicious Network model
Time(s) vs Number of Packets Dropped

VII. CONCLUSION

MANET has so many types of attacks which are to be addressed. One group of attacks called malicious packet dropper has been addressed in this paper. This group contains attacks such as black hole, grey hole and worm hole attack and behaves by dropping the packets or diverting the packets to the wrong node thereby by affecting adversely the performance of MANET. The main purpose of this paper is to improve the network performance of MANET, Which was achieved using the proposed approach called two diffie-helman packets approach to detect and prevent malicious packet dropper attack in MANET. The results have shown the effectiveness of the proposed approach compared to the existing system.

VIII. REFERENCE

1. Rutuja Shah et al., "Mitigating malicious attacks using trust based secure BEFORE Routing strategy in Mobile Ad hoc networks" journal of computing and information Technology, Vol. 24, No. 3, September 2016, pp. 237-252.

2. Yaser Khamaysel at al., "Malicious nodes detection in MANETs: Behavioural analysis approach." Vil. 7, N0. 1, January 2012, pp. 116-125

3. N. K. Gupta and K. Pandey, "trust based Ad hoc on Demand Routing Protocol for MANET", Sixth International IEEE conference on contemporary computing (IC3), 2013, pp. 225-231

4. P. N. Karthick and R. Bamalakshmi., " Detection and Prevention of the malicious packet dropping using blow fish Algorithm in Wireless Ad hoc Network", International journal of emerging Technology in Computer Science and electronics, Vol. 21, Issue. 3, April 2016

5. Krishnaveni Nunna et al., "truthful detection of packet dropping attack in MANET"., Journal of Emerging Technologies and Innovative Research, Vol. 3, Issue. 10, October 2016

6. S. Madhurikkha and R. Sabitha., "Detection of Malicious packet Droppers in MANET based on legitimate routing Information"., Journal of Chemical and pharmaceutical sciences, Vol. 9, Issue. 3, September 2016

7. Akansha Shrivastava and Ekta Chauhan., "Zone based Path Routing approach for detection and prevention of malicious behaviour of the node in MANET." ICTACT Journal on communication Technology, Vol. 7, Issue. 3, September 2016

8. V. Balakrishnan and V. Varadharajan., " Short Paper: Fellowship in Mobile Ad hoc Networks", First IEEE International Conference on Security and privacy of Emerging Areas in Communications Networks (SecureComm 2005), pp. 225-227, 2005

9. K. S. Sujatha et al., "Design of Genetic Algorithm based IDS for MANET" IEEE International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012

10. K. Bradley et al., "Detecting disruptive routers: a distributed network monitoring approach" IEEE Symposium on Network, Vol. 12, No. 5, pp. 50-60, 1998

11. U. Venkanna and R. L. Velusamy., "Black hole attack and their counter measure based on trust management in manet: A survey." Third International Conference on Advances in recent Technologies in communication and computing, pp. 232-236, 2011