Enhancing the Performance of MANETs using Period based Defense Mechanism

C.Logeshwari
Department of Computer Science and Engineering
Kalaignar Karunanidhi Institute of Technology
Coimbatore, India

N.Gugha Priya, Assistant Professor
Department of Information Technology
Kalaignar Karunanidhi Institute of Technology
Coimbatore, India

ABSTRACT

Mobile Ad hoc NETwork (MANET) is a group of mobile nodes and need not be a centralized infrastructure in the network. Every single mobile node acts as both transmitter and receiver then it communicates directly if the nodes are in the same network. Intrusion detection is a software application that monitors network and finds when unauthorized users enters the network. To protect MANET from the attackers, designed an intrusion detection system is called Enhanced Adaptive ACKnowledgement (EAACK). When data packets are sent from source to destination the problems such as receiver collision, limited transmission power and false misbehavior report occurs. EAACK can also detect these problems by using the schemes- ACK, Secure ACK and Misbehavior Report Authentication. The data flooding attack causes Denial of Service (DoS) attacks by flooding many data packets in the network. Therefore, in this paper we propose a scheme called Period-based Defense Mechanism (PDM) to avoid data flooding in the network. Then consider the performance of PDM scheme by measuring the throughput and also to improve the performance. The simulation results show that the performance of MANET is increased based on throughput and delay.

Keywords

Mobile Ad hoc NETwork (MANET), Advanced Encryption Standard (AES), Digital Signature Algorithm (DSA), data flooding, throughput, Period-based Defense Mechanism (PDM).

1. INTRODUCTION

MANET is a wireless decentralized network infrastructure and the mobile nodes can communicate with each other when the nodes are in the same communication range. Otherwise, depending upon the neighbor’s node, it transfers the information to other nodes then every mobile node can move freely in the network. The intrusion detection system is mainly used to guide the network and detects malicious attackers during the network communication. MANET consists of single-hop network and multi-hop network. In single hop, within the same network all nodes communicate with each other [5]. In multi-hop, nodes transmit based on the intermediate node, when nodes are in out of the network. EAACK is designed for defending mobile ad hoc network and it handles three problems: receiver collision, limited transmission power and false misbehavior report [1].

In the previous work, both RSA and DSA scheme was implemented to compare their performance and data communication has been done between the two users in the digital signature. The digital signature is used to make certain confidentiality, authentication, data integrity and non repudiation of MANETs. To facilitate the performance measure of EAACK scheme two metrics were used such as Packet Delivery Ratio (PDR) and Routing Overhead (RO).

The simulation results shows that DSA scheme always fabricates a little less network overhead than the RSA scheme. By using RSA, the network produces more malicious nodes so it is not preferable for MANETS. Hence, we find DSA is more enviable digital signature scheme. In MANET during the data transmission attackers will be detected, so to minimize the attackers and also to reduce the network overhead caused by digital signature we use AES and DSA algorithm. To study the potential of implementing a key exchange mechanism and to eradicate the requirement of pre distributed keys we use hybrid cryptography techniques. Here, data flooding occurs while sending many data packets continuously from source to destination. Hence, this paper proposes a PDM scheme to adjacent data flooding attacks.

2. PROTOCOL DESIGN OF EAACK

In this section, EAACK contains three main parts, specifically ACK, secure ACK(S-ACK) and misbehavior report authentication (MRA) to protect MANET from attacks. Consider that link between all nodes in the network is bidirectional. Both the source node and destination node are not malicious for each communication process. After that all acknowledgement packets are desired to be digitally signed by its sender and verified by its receiver.

2.1 ACK

ACK is fundamentally an end-to-end acknowledgement scheme because if the source node sends the request then destination node should send acknowledgement within the particular time period, the packet transmission from source S to destination D is successful as shown in the Figure1. Otherwise the source node S, move about to S-ACK scheme by transferring data packet to identify the misbehaving nodes in the network. Also, it performs as a branch of the hybrid scheme in EAACK, it is intending to reduce network overhead when no network misbehavior is detected.

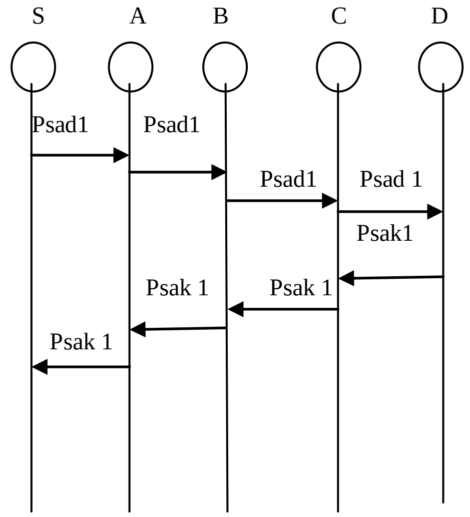

Fig 1: ACK scheme

2.2 S-ACK

In this scheme, the successive nodes work in a set together to identify misbehaving nodes in the network. As shown in the Figure2, the successive nodes (A, B, and C) to find misbehaving nodes. Node A sends S-ACK data packet to node B and node B forwards the same packet to node C. After receiving data packet Psad1 node C send acknowledgement to node B then, node B forwards the Psak1 to node A. If node A does not receives the acknowledgement within the particular time period, then both nodes B and C are defined as malicious and also a misbehavior report will be produced by node A and sent to the source node S in the network. Moreover, the source node instantaneously convicts the misbehavior report, EAACK needs the source node to move to MRA scheme and substantiate the misbehavior report. This is an essential step to distinguish false misbehavior report.

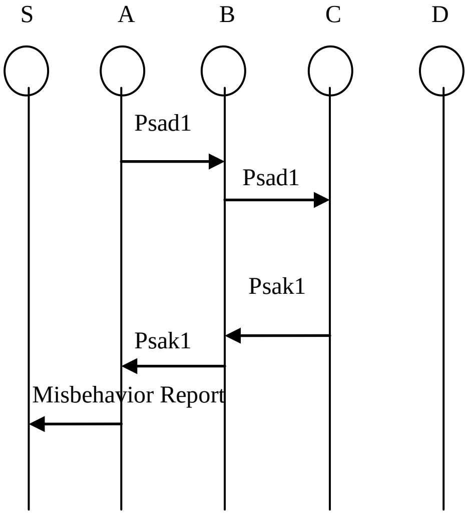

Fig 2: Secure-ACK scheme

2.3 MRA

The Misbehavior Report Authentication (MRA) scheme is intended to solve the problem when it fails to find misbehaving nodes with the occurrence of false misbehavior report [3] [4]. The malicious attackers falsely describe innocent nodes as malicious then, false misbehavior report can be produced by them. In this, the source node investigates its local information base and looks for different route to the destination node [6] [7]. If there is no path between two nodes, the source node sends DSR routing request to discover an additional route.

To avoid the misbehavior node, we adopt multiple routes to the destination node. If the reported packet was recognized, it explores the local information base and contrast when the destination node obtains an MRA packet. The node is safe when the reported packet is already received and it is a false misbehavior report and those who produced these reports distinct as malicious. Otherwise the misbehavior report is trusted and acknowledged. Moreover, the EAACK is accomplished to perceive malicious nodes even if the survival of false misbehavior report.

3. HYBRID CRYPTOGRAPHY TECHNIQUES

In this section, we describe about digital signature algorithm (DSA) and advanced encryption standard (AES) to reduce network overhead and also to minimize the attackers in the network.

3.1 DSA

In digital signature, destination sends file request and source node receives it. Data transfer will be done via shortest path and attacker may chance to occur then data loss will be there. If attacker detects many data gets lost. By using digital signature algorithm, each node request for private key and source node provides secret key to all the nodes to keep secure. Source will try to send data to which nodes providing the secret key. Then, remaining nodes are considered as malicious nodes since it does not send secret key. Therefore, shortest path is created between the non malicious nodes [8].

3.2 AES

AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. The main loop of AES performs the following functions are SubBytes(), ShiftRows(), MixColumns(), AddRoundKey().

The first three functions of an AES round are designed to thwart cryptanalysis via the methods of "confusion" and "diffusion." Diffusion means patterns in the plaintext are dispersed in the cipher text. Confusion means the relationship between the plaintext and the cipher text is obscured. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially MixColumns() and ShiftRows().This algorithm is mainly used to provide security for the secret information and also to reduce network overhead then the performance will be improved.

4. PERIOD - BASED DEFENSE MECHANISM

In this part, we focus on describing PDM to avoid flooding attack and also to improve the throughput in the mobile ad hoc network.

To protect the data flooding attack, the proposed PDM scheme used w time periods for the data transmission. This scheme ensures data packet floods at the last part of each stage to facilitate augment the throughput of burst traffic. We indicate v(n_{Sp} –n_{Dp}) as the variance of the number of acknowledged data packets for the source node (n_{Sp}) to the destination node (n_{Dp}) for the duration of time period T(i+1)-T(i+2). At this point, p represents the number of sessions acquired for data transmission. Then, throughput is defined as the ratio between the number of data packets sent by the sender and the number of data packets received by the receiver during the time period [2].

To find the variance limit of data packet floods from source to destination use the subsequent equation:

$$V_{limit}(n_{Sp}\text{-}n_{Dp})=ave(all)+h(n_{Sp}\text{ - }n_{Dp})$$

The steps for PDM scheme is following:

a) In MANETs, the different packets can be transfer through the mobile nodes by using links so that data flooding attacks can be avoided throughout the whole network.
b) The mobile node (n_u) compares the variance of acknowledged packets according to $Var_{limit}(n_{Sp}\text{-}n_{Dp})$, when the time period $T_{(i+2)}$ ends.
c) Each and every node maintains blacklist which is a list or register that can be deny someone effort in a certain amount of time. It checks whether the data packets of $D(n_{Sp}\text{-}n_{Dp})$ are available in the blacklist or not, when $Var(n_{Sp}\text{-}n_{Dp})$ is better than $Var_{limit}(n_{Sp}\text{-}n_{Dp})$.
d) If $D(n_{Sp}\text{-}n_{Dp})$ is present in the blacklist, the process ends and it will not be transmitted until reach the time period $T_{(i+3)}$. Otherwise, priority is decided by inversion of the number of acknowledged packets and mobile node processes based on priority.
e) The mobile node revises the blacklist by the greatest number of acknowledged packets using the time period.

5. PERFORMANCE EVALUATION

In this part, we concentrate on describing the simulation results of improving the performance and throughput of MANETs and comparing the performance of DSA and AES algorithm by using hybrid cryptography techniques. The hybrid cryptography techniques are AES and ECC (Elliptic Curve Cryptography).

5.1 Simulation Configurations

Our simulation is performed within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu9.10. The system is running on a laptop with Intel(R) Core(TM) i3-2330M CPU @ 2.20GHz and 4-GB RAM. In order to better compare our simulation results with other research works, we approved the default scenario settings in NS 2.34. The intention is to give more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670×670 m. The maximum hops permitted in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. For each scheme, we ran every network scenario three times and calculated the average performance.

5.2 Simulation Results

In figure3, when data packets are sent from source to destination many packets gets lost because forwarding node F will forwards all the packets when it receives from source node. If any node receives same packet more than once, it ignores it. To reduce the data loss, throughput will be calculated by:

$$\text{Throughput} = \frac{\text{Total number of packets received}}{\text{simulation time in seconds}}$$

By using the above formula, throughput has calculated as number of packets received by destination and simulation time in seconds. In figure1, X-axis denoted as time and Y-axis denoted as throughput. It shows that compared to previous work, throughput has been increased to improve the performance. In this simulation result, data loss was reduced.

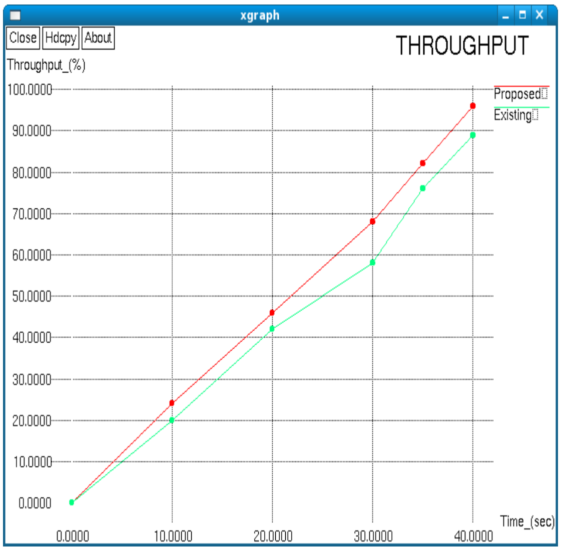

Fig 3: Throughput

In figure4, to reduce data loss in the network and to minimize the overhead in the network end to end delay will be calculated. Compared to previous work, delay has been decreased. In this, X-axis denotes the time in seconds and Y-axis denotes the packets in bytes. To calculate the delay formula is given by,

$$\text{Delay} = \frac{\text{Number of Packets Sent}}{\text{Simulation time in seconds}}$$

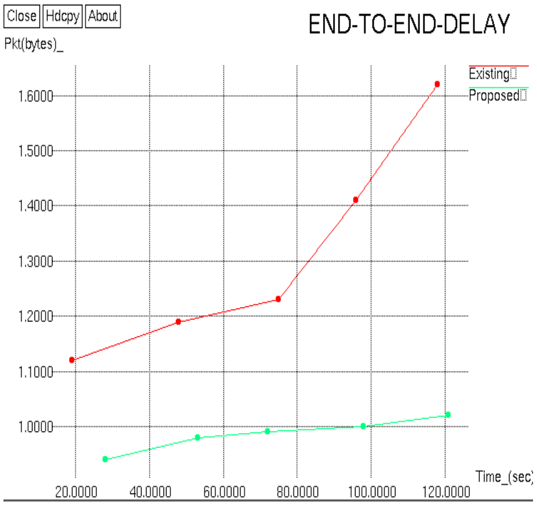

Fig 4: Delay

6. CONCLUSION AND FUTURE WORK

In this paper, protocol design of EAACK and digital signature algorithm has been implemented. The simulation results show that performance of MANET is increased based on throughput and delay. Because of the throughput and delay, data loss is reduced in the network. Future work is to implement the hybrid techniques such as AES and ECC and to compare both DSA and AES algorithm which is providing better performance. Also, to avoid data flooding attacks in MANET the PDM scheme is to be implemented.

7. REFERENCES

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, “EAACK—A Secure Intrusion-Detection System for MANETs” Member, IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013.

[2] Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, “Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks” , IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010.

[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehaviour in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[4] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting misbehaving nodes in MANETs,” in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[5] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[6] D. Johnson and D. Maltz, “Dynamic Source Routing in ad hoc wireless networks,” in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[7] G. Jayakumar and G. Gopinath, “Ad hoc mobile wireless networks routing protocol—A review,” J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[8] N. Nasser and Y. Chen, “Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network,” in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.