Indian Journal of Communication Engineering and Systems (IJCES)
Vol.2.No.1 2014 pp 32-36.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

A NOVEL IDS BASED EAACK FOR MANET

N.Tamil priya, Mr. K. C. Prabu Shankar
Dept.of Computer science engg.
St.Joseph's College of Engg. & Tech.
A.S.Nagar, Thanjavur
n.tamilpriyacse@gmail.com

ABSTRACT

There is a transition from Wired Network to Wireless Network. Owing to the improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades. Due to their natural mobility and scalability, wireless networks are always preferred since the first day of their invention. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly, It is the open medium to protect the attack by intrusion detection system. A new intrusion detection method called Enhanced Adaptive Acknowledgement (EAACK) method for MANET has been proposed. This method detects higher network based malicious attack. EAACK method is used to rectify malicious attack, to using the digital signature concept. But digital signature concept, to using pre distributed key. so easy to identify the key. improve the security to using claim check carry over algorithm. In this algorithm to use to identify the original packet, eliminate the duplicate packet.

Key Words : Mobile ad-hoc networks(MANET),Enhanced adaptive acknowledgement(EAACK), MANET solves this problem by allowing intermediate parties to rely data transmission.

1. INTRODUCTION

Mobile Ad-hoc networks is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. One of the major advantage of wireless network is its ability to allow data communication between different parties and still maintain their mobility. This communication is limited to the range of transmitter. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own.

This is achieved by dividing MANET into two types of network namely single-hop and multi hop. Single-hop network, all nodes within the same radio range communicate directly with each other. In multi hop networks nodes relay on their radio range. MANET does not required fixed infrastructure. Thus all the nodes are free to move randomly. MANET is capable of creating networks without help of a centralized infrastructure .The open medium and remote distribution on MANET makes it vulnerable to various types of attacks .for example due to the nodes, lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks.

2. BACKGROUND

2.1. An IDS in MANET

The open medium and wide distribution of nodes males MANET vulnerable to malicious attacks. In this case to implement the intrusion detection system concept to prevent the MANET from this attacks. IDS usually act as the second layer of MANET. If MANET can detect the attackers as soon as they enter into the networks. It will be able to completely eliminate the potential damages caused by the compromised nodes in first time. To prevent the MANET from this attack to use the Watch dog schema.

2.1.1 Watchdog schema

The aims of watchdog is to improve the throughput of networks with the presence of the malicious nodes .Watchdog is notifier. It just watch the entering into the networks node. watchdog node detect the malicious nodes only not prevent the malicious attacks. Watchdog schema fails to detect the malicious with the presence of the following 1.Ambigous collisions,2.Receiver collisions,3.Limited transmissions power, 4.False misbehavior report,5.Collisions 6.Partial dropping.

2.1.2. TWOACK

To overcome the watchdog schema drawback to use the TWOACK schema. TWOACK schema to solve the receiver collisions problem. How to overcome means, explain in following diagram

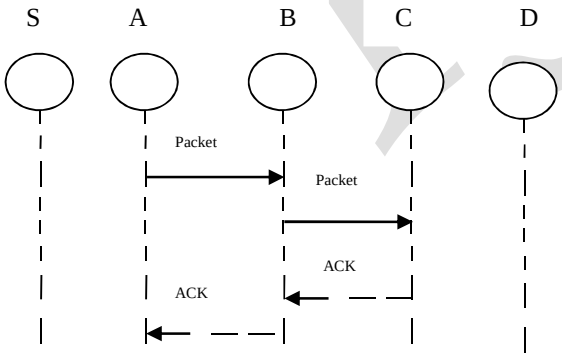

Fig 1. Solve the receiver collision problem

Source to destination A node sending msg to B node. B node sending packet c. c also sending the TWO ack before receiving the packet to source node..receiving the packet to destination, destination sending acknowledgement

2.1.3. AACK

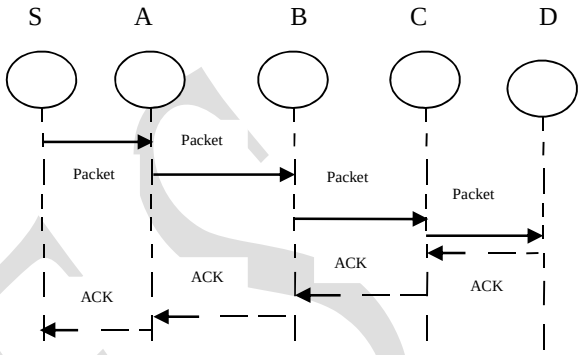

Fig 2.AACK

Source node S sends the packet. and intermediate node forward the packet. destination node D receive the packet. it required to sending acknowledgment packet to source node S, along reverse order of same route. but fail to detect the malicious nodes with the presence of the false misbehavior report and forged the ack packet.

2.1.4. Digital siganture

To prevent the malicious attacks to introduce the new intrusion detection concept is called Enhanced Adaptive acknowledgement. In this concept to using the Digital signature concept. how to perform the digital signature means, explain following diagram

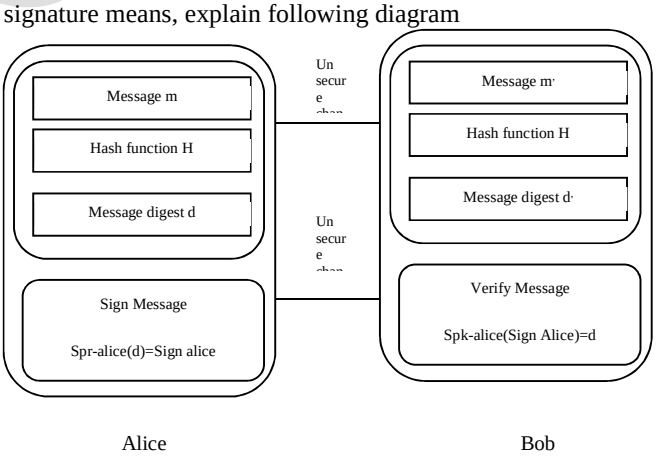

Fig 3. Digital signature

Digital Signature always been an integeral part of cryptography I history. The security MANET is defined as a combination of processes, procedures, system use to ensure the authentication, integrity and non repudiation of MANET. The original message is required in the signature verification algorithm after sending the packet from source to destination, the original message will digest computed through a pre agreed hash function H for every message M. the process can be described as

$$H(m) = d \quad (1)$$

Second the sender needs to apply its own private key pr_sender on the computed message digested. The result is a signature sig Alice with attached to message 'm' and sender secrete private key.

$$Spr\_sender(d) = Sigsender \quad (2)$$

the sender sending the message 'm' to destination receiver to compute the 'm' message to preagreed hash function to get the digest 'd'.

$$H(m') = d' \quad (3)$$

receiver can verify the signature by applying that the sender public key pk_sender an signature by using

$$Spk\_Sender(Sigsender) = d \quad (4)$$

If d = d' then it is safe to claim that the message m' transmitted through the unsecured channel.

Digital signature algorithm to using the pre distributed key, so attacker easy to identify the key. in digital signature algorithm not maintain the security, so to using the new algorithm called claim check carry over algorithm.

3. CLAIM CHECK CARRY OVER ALGORITHM

3.1 Claim Construction

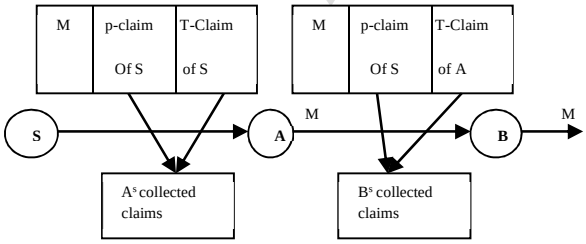

Fig 4. Claim construction

Two pieces of metadata are added to each packet (Fig. 3.1), the metadata are Packet Count Claim (P-claim) and Transmission Count Claim (T-claim). P-claim and T-claim are used to detect original packet. P-claim is added by the source and transmitted to later hops along with the packet. T-claim is generated and processed hop-by-hop. The source generates a T-claim and appends it to the packet. When the first hop receives this packet, it peels off the T-claim; when it forwards the packet out, it appends a new T-claim to the packet. This process is continues. Each hop keeps the P-claim of the source and the T-claim of its previous hop to detect attacks.

3.1.1 P-Claim

When a source node S sends a new packet m to a contacted node, it generates a P-claim as

P-claim:

$$S, Cp, t, H(m), SIGs(H(H(m)|s \mid Cp \mid t)) \quad (5)$$

Equation (5) is the p-claim,here t is the current time. Cp(CP-[1,L) is the packet count of S, which means that this is the Cp^{th} new packet S has created and sent to the network in the current time interval. S increases Cp by one after sending m out. The P-claim is attached to packet m as a header field, and will always be forwarded along with the packet to later hops. When the contacted node receives this packet, it verifies the signature in the P-claim, and checks the value of Cp. If cp is larger than L, it discards this packet; otherwise, it stores this packet and the P-claim.

3.1.2 T-Claim

When node A transmits a packet m to node B, it appends a T-claim to m. The T-claim includes A's current transmission count Ct for m and the current time t. The T-claim is

T-claim:

$$A,B,H(m),Ct, t, SIGA(H(A|B|H(m)| Ct \mid t)) \quad (6)$$

Equation (6) is the T-claim. B checks if Ct is in the correct range based on if A is the source of m. If Ct has a valid value, B stores this T-claim. In single-copy and multicopy routing, after forwarding m for enough times,

A deletes its own copy of m and will not forward m again.

In this P-Claim, T-Claim to identify the original packet, easy to avoid the duplicate packet, and increase packet delivery, improve the better performance compare to existing one.

4. PERFORMANCE EVALUATION

In this section, To concentrate on describing in simulation environment and methodology as well as comparing performances through simulation result comparison with EAACK schemes and claim check carry over algorithm.

A. Simulation Methodologies

In EAACK schema to rectify the malicious node to using the digital signature concept. digital signature concept to using pre distributed key. so easy to identify the key. To improve the security to using claim check carry over algorithm. claim check carry over algorithm to adding the P- claim, and T-Claim.in two claim to using identify the original packet.

1. *Scenario 1*

In this scenario, Digital signature to use the pre distributed key so attacker easy to identify the key. The purpose of this scenario to increase the security.

2. *Scenario II*

In this scenario, to use same key for complete process, so computational cost decrease, the purpose of this scenario to increase the computational cost.

3. *Scenario II*

In this scenario, When compare to Eaack method to decrease the performance and security. so propose this scenario to rectify the all the weakness.

A. Performance Evaluation

To provide the better result when compare to eaack method.

1. Simulation result I : *Scenario 1*

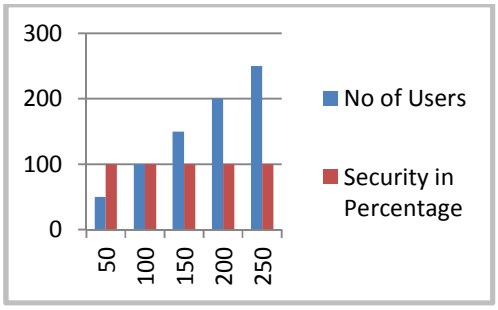

Fig 5-simulation result I-increase the security

In this scenario, Digital signature to use the pre distributed key .so attacker easy to identify the key. so The purpose of this scenario to increase the security. To use the p-claim and T-claim.in two claim to add the each packet, to identify the original packet. So security will be increase in fig 5.

2. Simulation result II : *Scenario 1I*

A node generates one signature for each newly generated packet. It also generates one signature for all its T-claims as a whole sent in a contact. As to signature verification, a node verifies the signature of each received packet. It also verifies one signature for all the T-claims as a whole received in one contact, so increase the computational cost in fig 4.2.

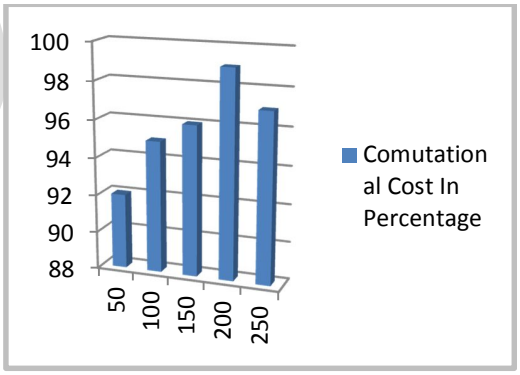

Fig 6. Simulation result II- increase the computational cost

Simulation result III : *Scenario III*

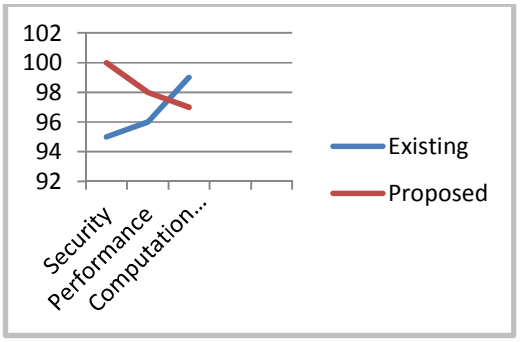

Fig 7..Simulation result III

In fig 7 to increase the security, performance and computational cost when compare to Eaack method.

5. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. EAACK method, to rectify malicious attack in network. But data is not secure in this process and also performance is decreased. In future work considered the data security and increase the performance, security. So to choose the Claim check carries over algorithm. in this algorithm to identify the original packet, and duplicate packet will be eliminate. so increase the network performance, increase the packet delivery ratio.

REFERENCES

[1] Qinghua Li, "To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks" in dependable and secure computing, vol. 10, no. 3, may/ june 2013

[2] 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

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

[4] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[5] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in *Proc. 2nd Conf. m-Bus.*, Vienna, Austria, Jun. 2003

[6] L. Zhou and Z. Haas, "Securing ad-hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

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

[8] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[9] 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

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

[11] 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.

[12]J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf. Perform., Comput., Commun.*, 2004, pp. 747–752.

[13] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[14] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[15] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666