ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Improved Adaptive Response for Mobile Ad hoc Network

P. Sethupriyan, R.Mohanraj

Assistant Professor, Bharath University, Chennai, Tamil Nadu, India

Assistant Professor, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT: The mobile ad hoc network (MANET) has been prevalent in various applications, together with some decisive undertaking applications, and as such security has become one of the major concerns in MANET. MANET is free to move independently in any direction, and will consequently change its links to other devices habitually. However the open medium and wide distributions of nodes make to an assortment of wicked attacks. In this paper, we propose and implement a new invasion recognition system named improved Adaptive response specially designed for MANET and Compared to all contemporary approaches. The results will be positive performances of WATCHDOG, S-TWOACK, and in the cases are recipient clash, inadequate diffusion control, and counterfeit misbehavior report.

KEYWORDS: MANET, Improved adaptive response.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. A MANET with the characteristics described above was originally developed for military purposes, as nodes are scattered across a battlefield and there is no infrastructure to help them form a network. An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. we have proposed a novel IDS named ACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power and false misbehavior report. IDS in MANET As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches Anantvalee and Wu presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and Adaptive Acknowledgment (AACK).

1) Watchdog*:* Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

2) TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed one of the most important approaches among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. The TWOACK scheme successfully solves the receiver Collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

3) AACK: a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TWOACK and an end-to-end acknowledgment scheme called Acknowledge.

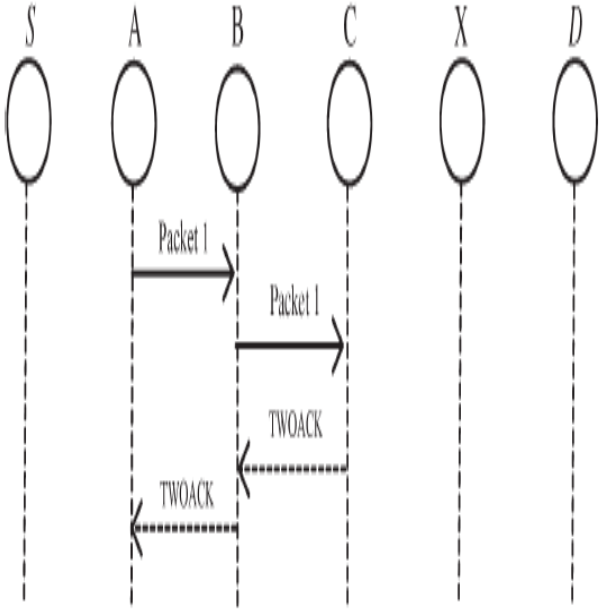

Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

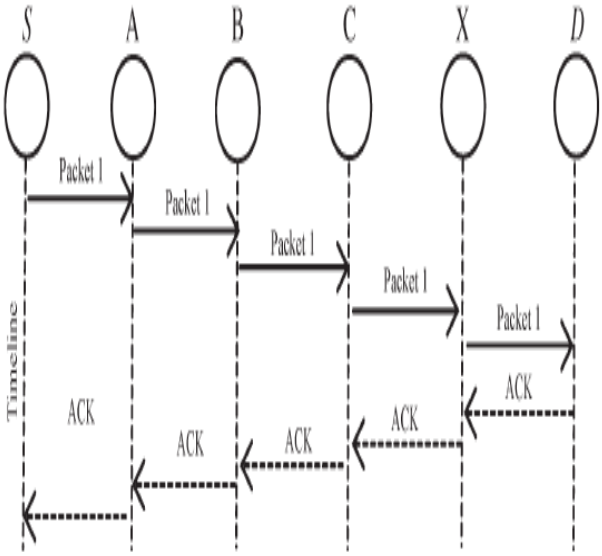

Fig.2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

II. LITERATURE SURVEY

2.1 A Survey on Intrusion Detection Systems in MANET [2]: Intrusion means any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusion Prevention is the primary defense because the primary step is to make the systems safe from attacks by using passwords, biometrics etc. Even if intrusion prevention methods are used, the system may be subjected to some vulnerability. So we need a second wall of defense known as Intrusion Detection Systems (IDSs), to detect and produce responses if necessary.

2.2 Enhanced IDS for Discovering Malicious Nodes in MANET [1]: Many intrusion detection systems have been proposed and most of them are tightly related to routing protocols, such as Watchdog/Pathrater and Route-guard. These solutions include two parts: intrusion detection (Watchdog) and response (Pathrater and Route-guard). Watchdog resides in each node and is based on overhearing. Through overhearing, each node can detect the malicious action of its neighbours and report other nodes. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance. They had we overcome the weakness of Watchdog and introduce our intrusion detection system called Ex-Watchdog.

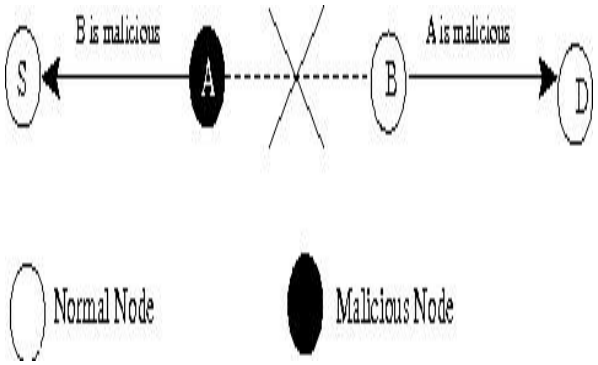

Fig 3.Malicious node

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

2.3 Secure Trust Metadata Management for MANET [3]: A trust management framework [2] is useful to ensure proper functioning of a mobile ad-hoc network (MANET). Trust metadata created by individual nodes, based on their observation of the behavior of other nodes in their vicinity, is required to be accessible to a trust authority (e.g., the network administrator) for prompt decision making (e.g., revoking malicious nodes). In this work, for security and scalability reasons, we propose a secure semantics-aware trust metadata management scheme to partition and store an information network of trust metadata of nodes in a MANET. That is, trust metadata is securely propagated to and stored at certain geographic locations inside the network itself, based on its semantics.

2.4 SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks[3]: This paper design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial of-Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

2.5 Dynamic Source Routing in Ad Hoc Wireless Networks [4]: This paper presents a protocol for routing in ad hoc networks that uses dynamic source routing. The protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates.

III. EXISTING SYSTEM

The network performance was identified by the received signal strength at the destination. The path from source to destination was vulnerable to spoofing attacks. There was no method proposed here to detect the presence of attackers. So overall throughput of the network was minimum and the network performance was degraded.

IV. PROPOSED SYSTEM

The EEACK consist of three major parts as ACK, SACK and MRA.

1. ACK: ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in ACK, aiming to reduce network overhead when no network misbehavior is detected.

2. SACK: The S-ACK scheme is an improved version of the TWOACK Scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

3. MRA: To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes two nodes.

By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. ACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

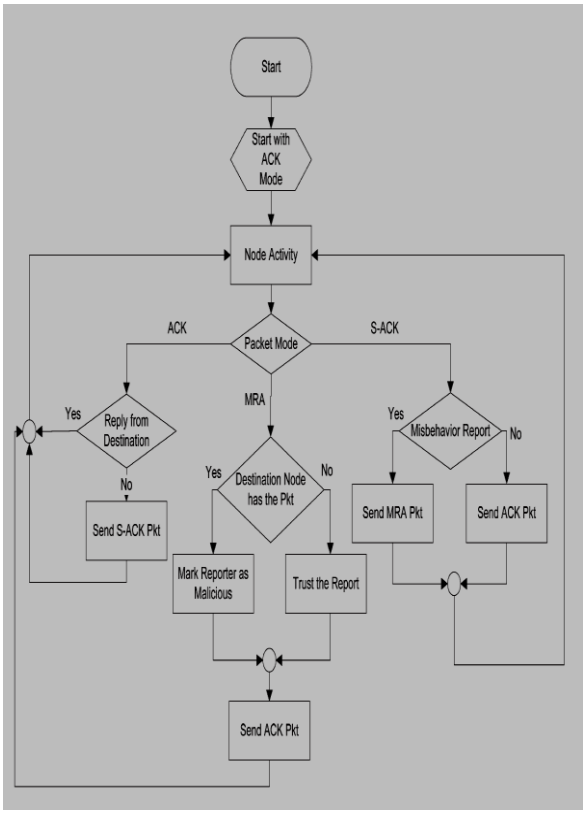

Fig 4: ACK Scheme

.

VI. CONCLUSION AND FUTURE WORK

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named ACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. To increase the merits of our research work, we plan to investigate the following issues in our future research:

1) Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;

2) Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of redistributed keys;

3) Testing the performance of ACK in real network environment instead of software simulation.

REFERENCES

[1] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[2] Anbuselvi S., Rebecca J., "A comparative study on the biodegradation of coir waste by three different species of Marine cyanobacteria", Journal of Applied Sciences Research, ISSN : 1815-932x, 5(12) (2009) pp.2369-2374.

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

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

[4] Bharatwaj R.S., Vijaya K., Rajaram P., "A descriptive study of knowledge, attitude and practice with regard to voluntary blood donation among medical undergraduate students in Pondicherry, India", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(S4) (2012) pp.602-604.
[5] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.
[6] Raj M.S., Saravanan T., Srinivasan V., "A modified direct torque control of induction motor using space vector modulation technique", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 20(11) (2014) pp.1572-1574
[7] 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.
[8] Rajasulochana P., Krishnamoorthy P., Dhamotharan R., "An Investigation on the evaluation of heavy metals in Kappaphycus alvarezii", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(6) (2012) pp. 3224-3228.
[9] 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.
[10] Jasmine M.I.F., Yezdani A.A., Tajir F., Venu R.M., "Analysis of stress in bone and microimplants during en-masse retraction of maxillary and mandibular anterior teeth with different insertion angulations: A 3-dimensional finite element analysis study", American Journal of Orthodontics and Dentofacial Orthopedics, ISSN : 0889-5406, 141(1) (2012) pp. 71-80.
[11] 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.
[12] 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.
[13] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[14] 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.
[15] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.
[16] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.
[17] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc. ACM Workshop Wireless Secur., 2002, pp. 1–10.
[18] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.
[19] B Karthik, TVU Kirankumar, MS Raj, E BharathKumaran,Simulation and Implementation of Speech Compression Algorithm in VLSI, Middle-East Journal of Scientific Research 20 (9), PP 1091-1092, 2013.
[20] A.Geetha, Face Recognition Using OPENCL, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , ISSN (Print) : 2320 – 3765, pp- 7148-7151, Vol. 3, Issue 2, Febuary 2014.
[21] A.Geetha, Universal Asynchronous Receiver / Transmitter (UART) Design for Hand Held Mobile Devices, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2231-5381, pp 25-26, Volume 3 Issue 1 No1 – January 2012.
[22] D.Sridhar raja, Comparison of UWB Band pass filter and EBG embedded UWB Band pass filter, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN 2278 – 8875,pp 253-257 ,Vol. 1, Issue 4, October 2012
[23] D.Sridhar raja, Performances of Asymmetric Electromagnetic Band Gap Structure in UWB Band pass notch filter, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 5492-5496, Vol. 2, Issue 11, November 2013
[24] Dr.S.Senthil kumar, Geothermal Power Plant Design using PLC and SCADA, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN 2278 – 8875,pp 30-34, Vol. 1, Issue 1, July 2012