ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

ENCHANCED ADAPTIVE ACK-PROTECTED INTERRUPTION DETECTION SYSTEM USING DIGITAL SIGNATURE FOR MANET

Dr N.Mahesh M.E.,Ph.D
Associate Professor, Dept. of Computer Science and Engineering,
Inst. Of Road and Transport Technology,
Erode-638 316.

Krishna Karthik.K
2nd Year, Master of Computer Science and Engineering,
Department of Computer Science and Engineering,
Inst. Of Road and Transport Technology, Erode-638 316.

***Abstract*— The migration to wireless network from wired net-work has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless net-works, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowl-edgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher mali-cious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.**

General Terms: **Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET).**

1. Introduction

Mobile Ad hoc NETwork (MANET) 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. Industrial remote access and control via wireless networks are becoming more and more popular these days [35]. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still main-tain their mobility. However, this communication is limited to the range of transmitters. 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. MANET solves this problem by allowing intermediate par-ties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other.

On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [10], [27], [29]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenar-ios like natural or human-induced disasters, military conflicts, and medical emergency situations

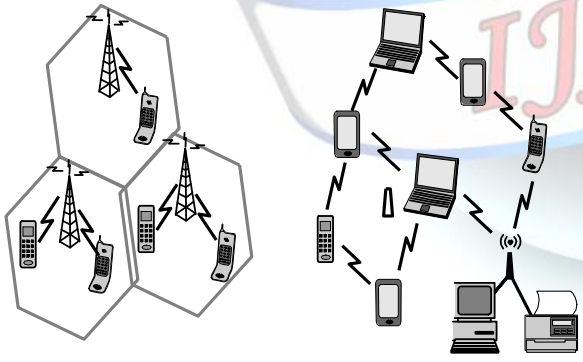
All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

2. MANET

A mobile ad hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing - catering to both nomadic and fixed users, anytime and anywhere



(a) Cellular Network (b) Mobile Ad Hoc Network

Fig 2.1 Cellular vs MANETS

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing - catering to both nomadic and fixed users, anytime and anywhere. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. For example, consider communication amongst soldiers in a battlefield, involving troops spread out over a large area. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in mobile ad hoc networks, wireless networks comprised of mobile computing devices communicating without any fixed infrastructure.

However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make 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.In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or noncooperative nodes into the network. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks.Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc

3.Existing System

The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this project, propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes,included a 2-b packet header in EAACK.

4.Proposed System

In this project developed for an effort to prevent the attackers from initiating forged acknowledgment attacks, here extended our research to incorporate digital signature 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. The proposed system uses message digest cryptographic hash function to detect the malicious node anywhere in the network.

5. Experimental Architecture and Implementation

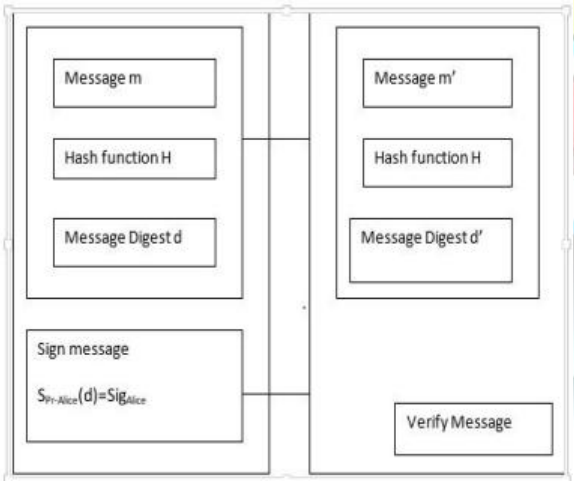


Fig 5.1 communication with digital signature

5.1 Network Formation

In this module we can construct a topology to provide communication paths for wireless adhoc network. Here the node will give the own details.
such as Node ID through which the transmission is done and similarly give the neighbor nodes details. Each node has the routing table for update its local information

5.2 Data Routing In Manet

In this module source node sends a encrypted message to destination, diffie hell man key exchange algorithm, a hybrid cryptography technique is proposed for secure and authenticated data transmission, key exchange mechanism is a part of diffie hell man key exchange algorithm.

5.3 EAACK- Acknowledgement Module

In this module the destination node send acknowledgement details. Set of nodes that have received the packet transmitted by node. In this module nodes send acknowledgement packet who received the packet from the source. In the reception and acknowledgment stage, successful reception of the packet transmitted by node is acknowledged through EAACK – ACK process.

5.4 EAACK – Sack Process (Ack based ids)

If source node doesn't receives a ACK packet, then EAACK results in secure acknowledgement process (SACK). The SACK mode is a three consecutive intermediate node verification process. The first intermediate node sends a packet to second node and then to third node. The third node sends a ACK to second node, if the second node doesn't sends ack to first nine in predefined time, the first node generates a misbehavior report and send to source node stating second and third node are malicious node.

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

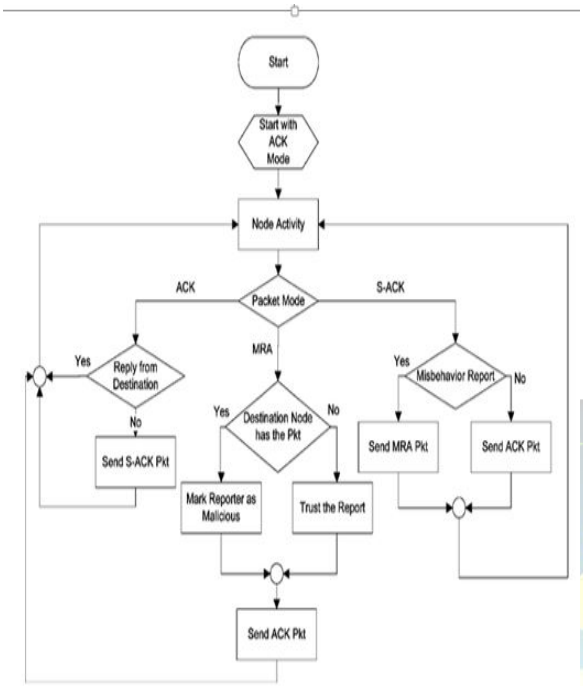


Fig 5.2 S-ACK Scheme

5.5 EAACK – MRA (Misbehavior Report Authentication)

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 (dynamic source routing) routing request to find another route.. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.

5.6 Digital Signature

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The development of cryptography technique has a long and fascinating history. The pursuit of secure communication has been conducted by human being since 4000 years ago in Egypt, according to Kahn's book in 1963. Such development dramatically accelerated since the World War II, which some believe is largely due to the globalization process. The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation. Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature. Digital signature schemes can be mainly divided into the following two categories.

1) Digital signature with appendix: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA).

2) Digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA

5.7 Graph Design Based Result

Graph is an essential part of display a result, so plot a graph to show a various result comparison with packets, throughput, energy efficient and etc.

Performance:

In this section, we concentrate on describing our simulation environment and methodology as well as comparing perfor-mances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes.

A. Simulation Methodologies

To better investigate the performance of EAACK under different types of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks.*Scenario 1:* In this scenario, we simulated a basic packet-dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watchdog, namely, receiver collision and limited transmission .

Scenario 2: This scenario is designed to test IDSs'

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

perfor-mances against false misbehavior report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

Scenario 3: This scenario is used to test the IDSs' perfor-mances when the attackers are smart enough to forge acknowl-edgment packets and claiming positive result while, in fact, it is negative. As Watchdog is not an acknowledgment-based scheme, it is not eligible for this scenario setting.

B. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM.In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide 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 allowed 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.In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics .

[1]Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

[2]Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

6.CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. A novel IDS named EAACK 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 extended our research to incorporate digital signature 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. In order to seek the optimal DSAs in MANETs Implemented both DSA and RSA schemes in our simulation. Eventually, arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs.

FUTURE WORK

To increase the merits of our research work, plan to investigate the following issues in our future research: Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature, examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys, Testing the performance of EAACK in real network environment instead of software simulation

REFERENCES

[1]. Elhadi M. Shakshuk, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs" VOL. 60, MARCH 2013.

[2] 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.

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

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

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

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[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] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowl-edgements in MANETs," inProc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[11] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, "Energy harvesting from piezoelectric materials fully integrated in footwear," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819, Mar. 2010

[12] 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.

All Rights Reserved © 2016 IJARTET