ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

Enhancing Key Management In Intrusion Detection System For Manets

Ms Shyama Sudarsan, Mrs Vinodhini, Dr S.Karthik

Abstract- **Manets are the ad hoc networks that are build on demand or instantly when some mobile nodes come in the mobility range of each other and decide to cooperate for data transfer and communication. Therefore there is no defined topology for Manets. Due to this lack of infrastructure and distributed nature they are more vulnerable for attacks and provide a good scope to malicious users to become part of the network. To prevent the security of mobile ad hoc networks many security measures are designed such as encryption algorithms, firewalls etc. EAACK is designed based on the Digital signature Algorithm (DSA) and RSA. those techniques have drawbacks due to the collusions of packets and distribution of keys between nodes becomes overhead. We propose a new alternate technique by developing a key management scheme and a secure routing protocol that secures on demand routing protocol such as DSR and AODV**.

Keywords- MANET, intrusion detection system, EAACK, key management

I. INTRODUCTION

Mobile ad hoc network (MANET) is a new emerging technology which enables users to communicate without using any fixed or physical infrastructure. These type of networks are suitable for several types of applications like military operations, emergency and rescue operations, wireless mesh and sensor networks, collaborative and distributed computing etc. In mobile ad hoc networks (MANET)[1] specific Intrusion Detection Systems (IDSs) are needed to safeguard them since traditional intrusion prevention techniques are not sufficient in the protection of MANET. Mobile Ad Hoc Networks are wireless networks in which the mobile nodes exchange information without the help of any predefined infrastructure. Intrusions are the activities that violate the security policy of system.

One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters Intrusion Detection is the process used to identify intrusions. Types of intrusion detection systems are based on the sources of the audit information used by each IDS, the IDSs may be classified into Host-base IDSs, Distributed IDSs and Network-based IDSs. The intrusion detection techniques are misuse detection that are based on known attacks and anomaly detection that are based on normal behaviour of a subject. The key management scheme is a hybrid key management scheme that uses both Symmetric Key Cryptography (SKC) for secure communication and Public Key Cryptography (PKC) to authenticate other nodes and to share a session key. Especially 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 [5], attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET’s distributed architecture and changing topology, traditional centralized monitoring technique is no longer feasible in MANETs. In the next section, we mainly concentrate on the papers already discussed about IDS required for understanding this survey topic.

II. FEATURES AND CHALLENGES

Features like autonomous terminal, distributed operation, multihop routing, dynamic network topology, fluctuating link capacity and light weight terminals. Routing protocol, security, medium access scheme ,energy management, quality of service ,self organization, protocol multicasting, scalability are some of the challenges that are taken into account for designing a MANET. Dynamic behavior, link instability, node mobility and frequently changing topology of MANET makes the routing a core issue. An effective routing algorithm helps to extend the successful deployment of mobile ad hoc networks.

Manuscript received Sep 15, 2012.

Shyama Sudarsan*, Computer Science and Engineering, Anna University, Chennai, SNS College of Technology., kollam,India,09489822889*

Vinodhini*, Computer Science and Engineering, Anna University, Chennai, SNS College of Technology.*

Dr.S.Karthik*, Computer Science and Engineering, Anna University, Chennai, SNS College of Technology. .Coimbatore,India,0422-2666264*

III. INTRUSION DETECTION SYSTEM IN MANETS

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, Intrusion Detection System (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 first time. In this section, we mainly describe three existing approaches, namely, Watchdog[17] , TWOACK[15] and AACK[25].

A) Watchdog: Marti et al. proposed a scheme named Watchdog that aims to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Pathrater[10][20][25]. Watchdog serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. If 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 pre-defined 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.

B) *TWOACK:* With respect to the six weaknesses of Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK[20] proposed by Liu et al. [15*]* is one of the most important one 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 links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route.

C) AACK: Based on TWOACK, a new scheme called Adaptive ACKnowledgement (AACK) was proposed. Similar to TWOACK, AACK is an acknowledgement-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

.

IV. RELATED WORK

A. EVALUATING AND COMPARISON OF INTRUSION IN MOBILE AD HOC NETWORK

Prevention methods like authentication and cryptography techniques alone are not able to provide the security. Intrusion detection can be classified in two classes [3] based on data collection mechanisms and based on detection techniques Based on detection techniques: there are three board categories: misuse detection, anomaly detection, and specification-based detection

B. MITIGATING ROUTING MISBEHAVIOR IN MOBILE AD HOC NETWORKS

Two techniques are used to improve throughput in an adhoc network in the presenceof nodes that agree to forward packets but fail to do so.Detect misbehaving nodes. One solution to misbehaving nodes is to forward packets only through nodes that share a priori trust relationship. Another solution to misbehaving [16] nodes is to isolate these nodes from actual routing protocols for the network. The techniques used are to detect the presence of nodes that agree to forward packets but fail to do so. Here watchdog is used, that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. The two techniques increases throughput and the overhead transmission.

C. NEW TRUST BASED SECURITY METHOD FOR MOBILE AD-HOC NETWORKS

Secure routing is the milestone in mobile ad hoc networks. Routing is always the most significant part for any networks. A trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. Trust management is a multifunctional control mechanism. It uses trust values to favor packet forwarding by maintaining a trust counter for each node[10].A trust based security protocol attains confidentiality and authentication of packets in both routing and link layers of MANETs. A node will be punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious.

D. AN INTRUSION DETECTION SYSTEM FOR MANET

An enhancement of the Watchdog/ Pathrater form of Intrusion Detection in Mobile wireless Adhoc networks (MANET).They describe about attacks mainly

- Route logic compromise

EG: Misrouting, Black Hole

- Traffic pattern distortion

EG: Packet Dropping, Packet Generation

- Routing protocols in ad-hoc networks
- Routing protocols in ad-hoc networks with security

E. DETECTING AND PREVENTING ATTACKS USING NETWORK INTRUSION DETECTION SYSTEMS

A Network Intrusion Detection System[21] is used to monitor networks for attacks or intrusions. The network is also a pathway for intrusion. It follows the signature based IDs methodology for ascertaining attacks. Its an alert device in the event of attacks directed towards an entire network. It successfully captures packets transmitted over the entire network by promiscuous mode of operation and compares the traffic with crafted attack signatures. It also incorporates functionality to detect installed adapters on the system, selecting adapter for capture, pause capture and clearing captured data is shown in the screen shots.

V. EXISTING SYSTEM

To introduce new approach to the preceding approaches of intrusion detection system EAACK was introduced using digital signatures and RSA concepts. EAACK is an acknowledgement based IDS. EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted.

VI. PROPOSED SYSTEM

As the existing approach had defects ,a new scheme can be proposed where a key management scheme for group based MANETs in which a group leader can generate, distribute, update and revoke keys in its group and a provable secure routing protocol. Proposed key management scheme neither depends on a central server nor is it fully distributed. Our key management system forms a decentralized system that combines both centralized key management as well as distributed key management so that it can combine merits of both methods. Proposed key management scheme is a hybrid key management scheme that uses both Symmetric Key Cryptography (SKC) for secure communication and Public Key Cryptography (PKC) to authenticate other nodes and to share a session key. We also proposed a secure routing protocol especially for On-demand routing protocol

VII. CONCLUSION

Packet dropping attack has always been a major threat to the security in MANETs. To increase the merits of the existing system the proposed is used and by using Public Key Cryptography (PKC)[16], nodes can negotiate the session key for secure communication that fulfills the requirement of confidentiality. Security analysis results show that protocol establishes a route secure from different kind of attacks such as reply attack, rushing attack, IP spoofing and man in the middle attack

REFERENCE

[1] S. Makki, N. Pissinou, H. Huang, “The Security issues in the adhoc on demand distance vector routing protocol (AODV)”, In Proc. of the 2004 International Conference on Security and Management (SAM’04), pp.427-432

[2] N. Komninos, D. Vergados and C. Douligeris, “Detecting Unauthorized and Compromised Nodes in Mobile Ad-Hoc Networks”, Journal in Ad Hoc Networks, Elsevier Press, Vol. 5, (3), April 2007, pp. 289-298.

[3] Kashan Samad, Ejaz Ahmed, Waqar Mehmood: MultiLayer Cluster-based Intrusion Detection Architecture for Mobile Ad Hoc Networks using Mobile Agents , Hi Optical Networks and Enabling Technology (HONET), Islamabad, Pakistan, Dec 28-31, 2004.

[4] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha “Threshold-based intrusion detection in ad hoc networks and secure AODV,” Ad Hoc Networks, Vol. 6, Issue No. 4, pp. 578-599. June 2008.

[5]. N. Mohammed, H.Otrok, L. Wang, M. Debbabi, and P.Bhattacharya, “A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in Manet,” Proc.IEEE Wireless Comm. and Networking Conf. (WCNC), 2008.

[6] Bin Yang, Jianhong Yang, JinwuXu, Deben Yang. Hybrid Cluster-head selected algorithm for wireless sensor network [*J*]. Application Research of Computers, 2008.4, 4(25): 1-3.

[7]S. Vasudevan, J. Kurose, and D. Towsley, “Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2004.

[8]K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, J.-B. Viollet, "Which Wireless Technology for Industrial Wireless Sensor Networks? The Development of OCARI Technol," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 4266-4278, Oct 2009.

[9] R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Network Security", Lecture Notes in Electrical Engineering, vol. 127, pp. 659-666, Springer, 2012 – here1

[10]R.H. Akbani, S. Patel, D.C. Jinwala. “DoS Attacks in Mobile Ad Hoc Networks: A Survey”, the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012. – here1

[11]T. Anantvalee and J. Wu. A Survey on Intrusion Detection in Mobile Ad hoc Networks. In Wireless/Mobile Security, Springer, 2008.

[12] N. Nasser and Y. Chen. Enhanced Intrusion Detection Systems For Discovering Malicious Nodes in Mobile Ad Hoc Network, In Proceedings of IEEE International Conference On Communication, Glasgow, Scotland, June 24 – 28, 2007.

[13] A. Patcha and A. Mishra. Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad hoc Networks. In the Proceedings of Radio and Wireless Conference, pp. 75-78, 2003.

[14] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis. Secure Routing and Intrusion Detection in Ad hoc Networks. In the Proceedings of 3rd International Conference on Pervasive Computing and Communications, pp. 191-199, 2005.

[15] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. In the Communications of ACM, vol. 21, pp. 120-126, 1978.

[16] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, S. Lanceros-Mendez, "Energy Harvesting From Piezoelectric Materials Fully Integrated in Footw," IEEE Trans. on Industrial Electronics, vol. 57, no. 3, pp. 813-819, March 2010.

[17] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, A. Mahmoud. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, pp. 273-282, 2009.

[18] K. Stanoevska-Slabeva and M. Heitmann. Impact of Mobile Ad-Hoc Networks on the Mobile Value System. 2nd Conference on m-Business, Vienna, June 2003.

[19] A. Tabesh, L. G. Frechette, "A Low-Power Stand-Alone Adaptive Circuit for Harvesting Energy From a Piezoelectric Micropower Genera," IEEE Trans. on Industrial Electronics, vol. 57, no. 3, pp. 840-849, March 2010.

[20] M. Zapata and N. Asokan. Securing Ad hoc Routing Protocols. In the ACM Workshop on Wireless Security, pp. 1-10, 2002.

[21] L. Zhou and Z. Haas. Securing Ad-hoc Networks. In the IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, 1999.

[22] Jin-Shyan Lee, "A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 4, pp. 1835-1841, April 2008.

[23] J. Parker, J. Undercoffer, J. Pinkston and A. Joshi. On Intrusion Detection and Response for Mobile Ad hoc Networks. In the Proceedings of IEEE International Conference on Performance, Computing, and Communications, pp. 747-752, 2004.

[24] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, A. Mahmoud. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, pp. 273-282, 2009.

[25] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis. Secure Routing and Intrusion Detection in Ad hoc Networks. In the Proceedings of 3rd International Conference on Pervasive Computing and Communications, pp. 191-199, 2005.

[26]Elhadi M. Shakshuki, *Senior Member, IEEE*, Nan Kang and Tarek R. Sheltami, *Member, IEEE.* EAACK – A Secure Intrusion Detection System for MANETs.26april2012.

Ms. Shyama Sudarsan is pursuing Masters Degree Program in Computer Science and Engineering in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University-Chennai, Tamilnadu, India. She received the BTech degree from Mahathma Gandhi University in 2011. Her research interests include Mobile Ad-Hoc Network and wireless systems. She published paper in international journal and conferences. She is an active member of CSI.

Mrs.Vinodhini.B is presently an Assistant Professor in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University- Coimbatore, Tamilnadu, India. She received the M.E degree from the Avinashilingam University, Coimbatore and currently doing Ph.D in Anna University-Coimbatore. Her research interests include Computer Networks, Mobile Computing and Wireless Communications. She published papers in International and National Conferences.

Professor Dr.S.Karthik is presently Professor & Dean in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University- Coimbatore, Tamilnadu, India. He received the M.E degree from the Anna University Chennai and Ph.D degree from Ann University of Technology, Coimbatore. His research interests include network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet security architectures and active defense systems against DDoS attacks. Dr.S.Karthik published more than 35 papers in refereed international journals and 25 papers in conferences and has been involved many international conferences as Technical Chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.