ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Digital Signature Adaptive Acknowledgement

Uppalapati Srilakshmi
Research Scholar,
Department of Computer Science & Engineering,
Acharya Nagarjuna University,
Guntur, AP, India.

Dr.Bandla Srinivasa Rao
Research Guide,
Department of Computer Science & Engineering,
Acharya Nagarjuna University,
Guntur, AP, India.

Abstract:

Mobile Ad Hoc Network (MANET) is a collection of nodes that are configured automatically without having a fixed infrastructure. Since the nodes in MANET are resource constrained the network is vulnerable to various kinds of attacks. Due to the ubiquitous nature of the network it is widely used in real world applications. Real world applications are switching from traditional networks to MANETs due to the utility of such network. Moreover MANET can be used in case of emergencies where fixed infrastructure networks are not available. Securing MANET communications is to be given paramount importance. The nodes in MANET play two roles such as transmitter and receiver. Intrusion detection system plays a vital role in protecting MANET communications. Many IDSs came into existence. However, they can be further improved. Recently Shakshuki et al. proposed EAACK that is an IDS based on acknowledgement in this paper we propose and implement an IDS that provides fool proof security to MANET besides improving in packet delivery ratio, delay and routing performance. Our simulations using NS2 revealed that the proposed IDS can secure MANET communications.

Index Terms:

Security, Mobile Ad Hoc Network (MANET), intrusion detection.

RELATED WORKS:

MANET routing protocols assume that the nodes in MANET cooperate with each other. This assumption lets adversaries exploit vulnerabilities of MANET to launch various attacks. To address this issues MANET communications are secured using an intrusion detection system that can eliminate potential risks caused by the nodes which are compromised and used as vehicle for making attacks. This section reviews literature on IDS in MANETs. Especially our work is closely related to the IDS such as Watchdog [1], TWOACK [2], AACK [3], EAACK (DSA) [4], EAACK (RSA) [4], and A3ACKs [11] in one way or other.

Watchdog:

It was proposed in [1] which improved throughput in MANET besides securing communications. It has two parts namely Watchdog and Pathrater. The former serves as an IDS while the latter is meant for helping routing protocols for tracing misbehaved nodes and avoids them in future transmissions. The IDS part of Watchdog overhears next hop's transmission. If the next hop is not able to transmit data in certain time, it maintains a failure counter. Based on the pre-defined threshold the node which fails to forward packets repeatedly the node is deemed to be misbehaving node. Watchdog is capable of detecting malicious nodes but not the links. However, in the presence of the ambiguous collisions, receiver collisions, limited transmission power, false misbehaviour report, collusion and partial dropping the Watchdog cannot detect malicious nodes in MANET. To overcome these drawbacks many IDS schemes came into existence [5] and [6].

DRAWBACKS OF WATCHDOG:

The three important watchdog limitations in detecting malicious nodes are in the presence of receiver collision, limited transmission power, and false misbehaviour report. These three are overcome in EAACK [4] where was enhanced in this paper further to reduce routing overhead by implementing hybrid cryptosystems. The receiver collision occurs when two nodes simultaneously send packets to other node. As shown in Figure1, both B and X send packet 1 and packet 2 respectively to node C at the same time. This problem is known as receiver collision problem. The second problem is limited transmission power. As described in Watchdog IDS, a node overhears the next hop node to know whether packet transmission is successful.

To facilitate the one hop node limits its transmission power intentionally to enable the other node to overhear it at the cost of its capacity to forward it to next hop. The false misbehaviour report problem occurs when node A sends a false report to sender node. This is done even though B sends packet to C successfully. It does mean that the node A is misbehaving and the IDS like Watchdog is not able to detect it. However, EAACK and our solution can detect it as well. Moreover our solution in this paper overcomes the RO problem of EAACK by using KEM. Before presenting our scheme let us have a revisit of other acknowledgement based schemes and their merits and demerits.

TWOACK AND AACK SCHEMES:

This scheme was proposed by Liu et al. [2] which resolve two drawbacks of Watchdog such as receiver collision and limited transmission power. Unlike Watchdog [1], the TWOACK scheme detects misbehaving links. It needs acknowledgement for every packet sent over three consecutive nodes when it is in transit from source to the destination. Each node, when it retrieves a packet, should acknowledge the fact to the node that two hop away from the node down the route. This phenomenon is visualized in Figure 2. Node A sends packet to node B. Then B sends it to C. When C receives packet, it is supposed to acknowledge this fact to node A by sending a TWOACK packet. This will confirm to A that the packet has reached C. If this does not happen in given time limit, both B and C are doomed to be malicious.

AACK scheme proposed by Sheltami et al. [3] on the other hand is an end to end acknowledgement scheme that increases throughput further besides reducing network overhead. It is the combination of TWOACK and ACK schemes. As can be seen in ACK scheme of Figure 2, it is evident that the source nodes send a packet and that reaches destination. However, the acknowledgement is from destination to the source making it an end-to-end acknowledgement. When this is done in some pre-defined time limit, the packet transmission is considered successful. If not, the scheme switches to TACK (similar to TWOACK) thus reducing network overhead. The problem with Watchdog, TACK, TWOACK, and AACK they heavily depend on acknowledgement packets for successful intrusion detection. However, they may fail when acknowledgement packets are fake due to malicious attacks launched by attackers. To overcome this problem EAACK [4] came into existence.

PROPOSED SYSTEM:

Shakshuki et al. [4] proposed this scheme which makes use of digital signature besides an enhanced adaptive acknowledgement scheme. The digital signature can achieve the security features such as authentication, integrity and non-repudiation in MANETs. There are two kinds of digital signatures used in EAACK. They are namely digital signature with message recovery (RSA) and digital signature with appendix (DSA). EAACK with these two are compared with experimental results. EAACK can solve three problems of Watchdog. They are false misbehaviour, receiver collision and limited transmission power. These three problems are illustrated in Figure 1. The solution of EAACK has three parts namely ACK, secure ACK, and Misbehaviour Report Authentication (MRA). EAACK uses 2-b packet header in order to distinguish various packet types. It assumes the links to be bi-directional. ACK is the end-to-end data transmission scheme while the S-ACK is an improved version of TWOACK. The working principle of S-ACK is that every three consecutive nodes work together for malicious node detection. When source node obtains misbehaviour report, it trusts it simply. Here the MRA comes into picture which is meant for malicious node detection in the presence of false misbehaviour report generated by attackers.

To overcome the problem of false misbehaviour problem source node finds an alternative route to destination and sends MRA packet to destination node. On receiving this packet, the destination node verifies whether the said packet has been received. If that is already received, the source node concludes that the misbehaviour report it received was false. This proves that EAACK is able to detect malicious nodes even in the presence of false misbehaving report attacks. However, it believes the acknowledgement packets are genuine. This problem is overcome by EAACK by introducing digital signature usage into the IDS scheme. With this all packets of EAACK scheme needs to be signed digitally. As the digital signature helps in using public key cryptography, it is possible that fake acknowledgements initiated by adversaries can be detected. Based on EAACK the proposed system is built to be fool proof in providing security to MANET.

CONCLUSION AND FUTURE WORK:

In this paper we studied the problem of security in MANETs. Intrusion detection is one of the counter measures for security problems in such networks.

The nodes in the network are self configured and there is no fixed infrastructure available. The nodes are highly vulnerable to attacks. Traditionally intrusion detection systems were playing a major role in protecting networks. However, the traditional intrusion systems that work for wired networks are not suitable for wireless networks. Therefore it is essential to have IDS specific to MANET. Many researchers contributed towards building IDS for MANET. EAACK is one such IDS came into existence recently. In this paper we proposed and built an IDS to secure communications in MANET. Our system not only secures communications but also improves performance. In the presence of malicious nodes also, our proposed IDS performs better than existing ones. Besides improving security, our system also exhibits performance improvements in terms of packet delivery ratio, routing and delay performance. We made extensive simulations using NS2 which reveal the usefulness of our system. The empirical results are encouraging.

REFERENCES:

[1] 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.

[2] J.-S. Lee, “A Petri net design of command filters for semiautonomous mobile sensor networks,” IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[3] Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki, “Implementation of A3ACKs intrusion detection system under various mobility speeds”, ScienceDirect, 5th International Conference on Ambient Systems, vol. 32, pp.571-578, 2014.

[4] Ehsan Amiria*, Hassan Keshavarzb, Hossein Heidaric, Esmaeil Mohamadid and Hossein Moradzadehe. (2014). Intrusion Detection Systems in MANET: A Review. p454-459.

[5] J.-S. Lee, “A Petri net design of command filters for semiautonomous mobile sensor networks,” IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[6] A. Patcha and A. Mishra, “Collaborative security architecture for black hole attack prevention in mobile ad hoc networks,” in Proc. Radio Wireless Conf., 2003, pp. 75–78.

[7] Amin Hassanzadeh a, Radu Stoleru a,Michalis Polychronakis b and Geoffrey Xie. (2014). RAPID: Traffic-agnostic intrusion detection for resource-constrained wireless mesh networks. www.elsevier.com. p2-17.

[8] Amin Hassanzadeh, Ala Altaweel and Radu Stoleru. Traffic and resource aware intrusion detection in wireless mesh networks. www.elsevier.com. p19-41, 2014.

[9] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ahmed Patel. (2013). An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. p2106-2127.

[10] Sergio Pastrana a,Aikaterini Mitrokotsa b, Agustin Orfila a and Pedro Peris-Lopez. (2012). Evaluation of classification algorithms for intrusion detection in MANETs. p218-225.

[11] Da Zhang and Chai Kiat Yeo. (2011). Distributed Court System for intrusion detection in mobile ad hoc networks. p556-570.

[12] Sevil Sen, John A. Clark. (2011). Evolutionary computation techniques for intrusion detection in mobile ad hoc networks. p3442-3457.

[13] Bo-Chao Cheng a and Ryh-Yuh Tseng. (2011). A Context Adaptive Intrusion Detection System for MANET. p311-318.

[14] H. Chris Tseng a and B. Jack Culpepper b. (2005). Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators. p562-570.

[15] Hyunwoo Kima, Dongwoo Kimb and Sehun Kimc. (2005). Lifetime-enhancing selection of monitoring nodes for intrusion detection in mobile ad hoc networks. (AEÜ). p249-250.

[16] Lijun Qiana, Ning Songa and Xiangfang Lib. (2007). Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach. jnca. p309-330.

[17] Ningrinla Marchang a and Raja Datta. (2008). Collaborative techniques for intrusion detection in mobile ad-hoc networks. p509-523.

[18]Hadi Otrok, Noman Mohammed, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya. (2008). A game-theoretic intrusion detection model for mobile ad hoc networks. p709-721.

[19] Chandrasekar Ramachandran, Sudip Misra b, Mohammad S. Obaidat c. (2008). FORK: A novel two-pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks. p3856-3869.

[20] Adrian P. Lauf, Richard A. Peters and William H. Robinson. (2010). A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. p254-266.