

Eaack: eids for Manet Using Digital Signature

¹J.Ajitha, & ²N.Gnaneswara Rao

¹M.Tech Research Scholar,

²Professor, Department in CSE,

Vignan University, Vadlamudi, Andhra Pradesh.

Abstract:

In the past few decades the migration to wireless network from wired network has been a global trend. The functionality and features of MANET and the wireless medium also distribution of nodes makes MANET vulnerable to malicious attackers. A new improved technique EAACK (Enhanced Adaptive Acknowledgement) scheme designed for MANET was proposed for an Enhanced intrusion-detection system (EIDS) for MANETs. Here in this scheme we are using Digital Signature for providing more security. EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Keywords: Digital signature; DSA; EAACK; Mobile Ad hoc Network (MANET); EIDS.

1. INTRODUCTION

In the recent years, wireless technology has enjoyed a tremendous rise in popularity and usage, in the domain of networking. In MANETs, the participating

nodes do not rely on any existing network infrastructure. A mobile ad hoc network consisted of wireless nodes that can be rapidly deployed as a multi-hop packet radio network without the aid of any existing network infrastructure or centralized administration. Therefore, the interconnections between nodes are capable of changing on continual and arbitrary basis. Nodes within with in a radio range communicate directly, otherwise use intermediate parties to relay data transmissions. Ad hoc networks have a wide array of military and commercial applications. In these applications installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous.

Infrastructure network was destroyed. However, this flexibility introduces new security risks. Since prevention techniques are not enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions. Intrusion detection for MANETs is a complex and difficult task mainly due to the nature of

MANETs, their highly constrained nodes, and the lack of central monitoring points. so, new approaches need to be developed or else existing approaches need to be adapted for MANETs. In this paper suggest one of the intrusion detection for MANETs using EAACK.

2. BACKGROUND

2.1 Intrusion Detection in MANETs

In traditional wired networks many Intrusion Detection Systems has been proposed, where all traffic must go through hub, switches, routers, or gateways. Hence, Intrusion Detection Systems can be added to and implemented in these devices easily. On the other hand, Mobile Adhoc Networks do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it.

Furthermore, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information could be from a compromised node or a node that has outdated information. Thus, the current Intrusion Detection Systems techniques on wired networks cannot be applied directly to Mobile Adhoc Networks. Many Intrusion Detection Systems have been proposed to suit the characteristics of MANETs.

2.2 Overseer or Watchdog

The main of the Overseer mechanism is to improve the throughput of the network with the presence of malicious Nodes. The Overseer scheme is of two types namely

Overseer and pathrater. Overseer serves as intrusion Detection for Mobile Adhoc Network and responsible for detecting malicious node misbehavior in the network. Watchdog detects malicious node misbehaviors by listen in to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a predefined time period, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. At the same time, watchdog maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog scheme accuses the next-hop neighbor to be misbehaving.

2.3. Issues in Intrusion Detection System

Even though there are many proposed IDSS for wired networks, MANET's specific features make conventional IDSS ineffective and inefficient for this new environment. Researchers have been working recently on developing new IDSS for MANETs or changing the current IDSS to be suitable to MANETs. There are some new issues which should be taken into account when a new ID is being designed for MANETs.

- Lack of central points: MANETs do not have any entry points such as routers, gateways, etc. present in wired network.

These can be used to monitor all network traffic that passes through them. A node in a MANET can see only a portion of a network: the packets it sends or receives together with other packets within its radio range

3.RELATED WORKS

The Watchdog/Pathrater is a solution to the problem of selfish (or —misbehaving) nodes in MANET. The system introduces two extensions to the DSR algorithm to mitigate the effects of routing misbehavior: the Watchdog, to detect the misbehaving nodes and the Pathrater, to respond to the intrusion by isolating the selfish node from the network operation.

A. Intrusion Detection system in MANETS:

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, 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. IDSs usually act as the second layer in MANETs, and it is a great complement to existing proactive approaches and presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly

describe three existing approaches, namely, Watchdog, TWOACK and AACK.

B. watchdog:

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 Path rater. 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.

In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following researches and implementations have proved that the Watchdog scheme to be efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviors with the presence of

- ambiguous collisions,
- receiver collisions,
- limited transmission power,
- false misbehaviour report,
- collusion,
- Partial dropping.

C. TWOACK:

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.

The working process of TWOACK is demonstrated in Fig. 1, node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A.

TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement 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.

D. AACK:

It is based on TWOACK Acknowledgement (AACK) similar to TWOACK, AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (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.

Source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgement packets.

Problem Definitions

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power.

4. PROPOSED SYSTEM

A. Scheme description:

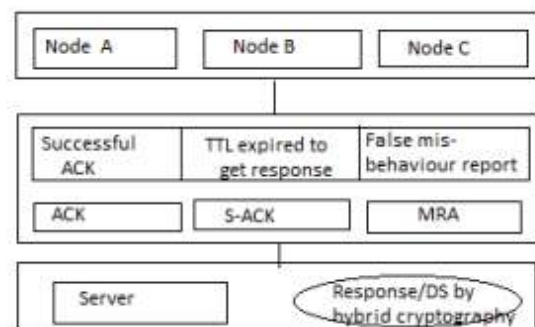


Fig 1. System Architecture

In this section, we describe our proposed Enhanced Adaptive Acknowledgement (EAACK) scheme in details. The approach described in this research paper is based on our previous work, where the backbone

of EAACK was proposed and evaluated through implementation. In this work, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely:

1. Acknowledge (ACK),
2. Secure-Acknowledge (S-ACK) and
3. Misbehavior Report Authentication (MRA).

B. AACK:

As discussed before, ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig.3, in ACK mode, node S first sends out an ACK data packet ad1 P to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D Successfully receives ad1 P, node D is required to send back an ACK acknowledgement packet ak1 P along the same route but in a reverse order.

C. S-ACK:

S-ACK scheme is an improved version of TWOACK scheme. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement 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. in S-ACK mode, the three consecutive nodes (i.e. F1, F2 and F3)

work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet to node F2.

D. MRA:

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route.

E. Digital Signature:

As discussed before, EAACK is an acknowledgement based IDS. All three parts of EAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviors in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement Packets, all of the three schemes will be vulnerable.

5.CONCLUSION

Packet dropping attack has been one of the major threats to MANETs. In order to prevent and eliminate packet dropping attack, various approaches have been proposed. But, none of the existing approaches address the problem when the attackers are smart enough to forge acknowledgement packet or send out false acknowledgement. EAACK stands for Enhanced Adaptive Acknowledgement mechanism. It is an enhancement on Adaptive Acknowledgement scheme (AACK). We extended AACK to a new level where EAACK is capable of detecting forged acknowledgement packet or false misbehavior report. EAACK has the highest packet delivery ratio. Even though EAACK produces a considerable amount of network overhead in some scenarios, we believe our proposed scheme is valuable when security is of top concern.

This paper can be considering the following issues in the future research:

- Avoid the requirement of pre distributed keys by a doping a key exchange mechanism
- Testing the performance in real network environment instead of software simulation.

REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE

Trans. Ind. Elec- tron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

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

[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, "Model- ing 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 IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand rout- ing protocol for ad hoc networks," in Proc. 8th

ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10] 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.

[11] 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.

[12] 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.

[13] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting forged acknowledgements in MANETs,” in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, “Mobile ad-hoc communications in AEC industry,” *J. Inf. Technol. Const.*, vol. 9, pp. 313–323, 2004.

[15] 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.

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

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile ad hoc networks,” in *Proc. 6th*

Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[18] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.

[19] 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.

[20] 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.

[21] 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.

[22] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, “Secure routing and intrusion detection in ad hoc networks,” in *Proc. 3rd Int. Conf. Pervasive Comput. Commun.*, 2005, pp. 191–199.

[23] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[24] 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.

- [25] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.
- [26] 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.
- [27] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
- [28] 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.
- [29] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.
- [30] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM Workshop Wireless Secur.*, 2002, pp. 1–10.
- [31] L. Zhou and Z. Haas, "Securing ad-hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.
- [32] Botan, A Friendly C++ Crypto Library. [Online]. Available: <http://botan.randombit.net/1098> IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013
- [33] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).
- [34] TIK WSN Research Group, The Sensor Network Museum—Tmote Sky. [Online]. Available:
- [35] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 7, pp. 1379–1387, Jul. 2008.