International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Review Paper on Preventing Forged Acknowledgement in Manets

Ajit N. Gedam[1], M. P. Wankhade[2]

[1]ME (Computer Network), Department of Computer Engineering, Sinhgad Collage of Engineering, Vadgaon (Bk), Pune. 411041, India

[2]Associate Professor, Department of Computer Engineering, Sinhgad Collage of Engineering, Vadgaon (Bk), Pune. 411041, India

Abstract: ***MANET is a group of mobile nodes that establish themselves into a network without any predefined infrastructure or centralized operation management. Mobile ad hoc networks are advantageous in situation such as flood or earthquake. MANET can quickly be established even though the network infrastructure is unavailable. It is very hard to detect and prevent forged acknowledgement. To prevent from forged acknowledgement, detection of misbehavior nodes plays an important role in MANETs. Dynamically changing topology, limited battery power and absence of centralized control in MANETs, make them vulnerable to detection of misbehavior nodes. Intrusion Detection System (IDS) is required to detect the misbehavior nodes before they can accomplish any significant damages to the network.***

Keywords: MANET; EAACK; DSA; RSA; Digital Signature; ACK; S-ACK; MRA

1. Introduction

By definition, a mobile ad hoc network is a constantly self-configuring, self-maintained infrastructure less network of mobile devices which are associated without wires. Mobile ad hoc network consists of mobile nodes. These mobile nodes, which can communicate with each other in bidirectional way having wireless transmitting and receiving factor in network, directly or indirectly.

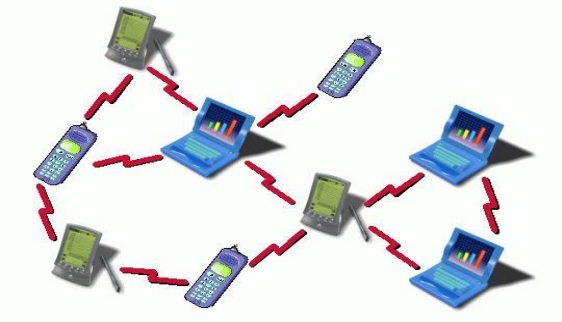

Figure 1.1: MANETs Architecture

Nodes are communicate with each other by using wireless network and various components and maintained its mobility. If nodes or components are not in the same range then use mobile ad hoc network. But to obtained this MANET which is divided into two different networks one is called as single hop network, in single hop network nodes which are present in the same range they can interact with each other directly, i.e. no any common nodes used in between. Another is multi-hop network, in which nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer possible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS). It is observed that most of existing routing protocols have ignored the aspect of network security, specially designed for MANETs. The main purpose is to propose a new advanced system, which specially designed for MANET's, which solves security issues during the packet transmission process. As in all acknowledgement base intrusion detection system, it is highly authenticated of all the acknowledgement packets.

2. IDS 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, 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, it will be able to completely eliminate the potential damages caused by compromised nodes at the first time. . In this section, mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive ACKnowledgment (AACK).

3. Forged Acknoledgement in MANETS

In fact, many OF the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern digital signature is adopted in scheme named Enhanced AACK (EAACK) to prevent forged acknowledgement. S-ACK modes of EAACK are digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet.

4. Literature Survey

In [2] this paper the author suggested scheme contains two major parts, termed watchdog and path rater, to detect and mitigate, respectively. Nodes operate in a promiscuous mode wherein the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the

packet. At the same time, it maintains a buffer of recently sent packets. 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 module accuses the next hop neighbor of misbehaving. Thus, the watchdog enables misbehavior detection at the forwarding level.

The Author In [3] his paper TWOACK scheme to detect misbehaving links by acknowledging every data packet transmitted over each three consecutive nodes along the path from the source to the destination.

In [4] the author invented 2ACK scheme which works like TWOACK with differences i) The data packet receiving node sends 2ACK packets as acknowledgment for a fraction of received data packets, while, in the TWOACK scheme, TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2ACK scheme better performance with respect to routing overhead. The 2ACK scheme has an authentication mechanism to make sure that the 2ACK packets are genuine. The 2ACK scheme suffers from false misbehavior report.

In [5] the author proposed Adaptive ACKnowledgment (AACK) scheme. The AACK is a network layer acknowledgment based scheme that may be considered as a combined system of an Enhanced-TWOACK (E-TWOACK), which detects misbehaving node instead of misbehaving link and an end-to end acknowledgment scheme, to reduce the routing overhead of TWOACK. The AACK mechanism may not work well on long paths that will take a significant time for the end to end acknowledgments. This limitation will give the misbehaving nodes more time for dropping more packets. Also AACK still suffers from the partial dropping attacks (gray hole attacks). It also suffers from false misbehavior report.

In [6] the author concentrate on security Enhanced Adaptive ACKnowledgement (EAACK) scheme which consists of three parts (i) Acknowledge (ACK) (ii) Secure-ACKnowledgement (S-ACK) (iii) Misbehavior Report Authentication (MRA). ACK is basically an end-to-end acknowledgement scheme. In ACK mode if destination node D successfully receives data packet, it send back an ACK acknowledgement packet along the same route but in a reverse order. Within a predefined time period, if node S receives ACK, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S ACK data packet to detect the misbehaving nodes in the route. S-ACK scheme is an improved version of TWOACK. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node as done in TWOACK. If the first node in a group does not receive S-ACK then it declare both second and third node as misbehaving nodes and send the report to source node. The source node do not immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. With MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

In [7] the author proposed EAACK2; in this acknowledgement packets received in S-ACK phase of EAACK are digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet. Both the EAACK and EAACK2 cannot detect partial dropping that is Gray hole, during the first phase node may drop packets as end to end acknowledgement take time.

In [8] the author analyzed the performance by introduction of digital signature in EAACK to prevent the attacker from forging acknowledgment packets. EAACK is consisted of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehavior Report Authentication (MRA). In EAACK, two of the six bits were used to flag different type of packets. In the proposed scheme it was assumed that the link between each node in the network is bi-directional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver. Summarized comparison of above reviewed techniques is tabularized as follows:

Table 1: Comparison of Various Approaches

Sr. No	Title	Extract Of The Paper	Routing Overhead	Detect False Misbehavior Report	Prevent Forged Acknowledgement	Solve Receiver Collisions Problem
1	"TWOACK: preventing selfishness in mobile ad hoc networks	TWOACK scheme to detect misbehaving links by acknowledging every data packet transmitted over each three consecutive nodes along the path from the source to the destination	Large	No	No	Yes
2.	An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs	The 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme.	Lesser Than TWOAK	No	Yes	Yes
3.	AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Detection Enhancement	The AACK is a network layer acknowledgment based scheme, detects misbehaving node instead of misbehaving link and an end-to end acknowledgment scheme, to reduce the routing overhead of TWOACK.	Lesser Than Above Techniques	No	No	Yes

Sr. No	Title	Extract Of The Paper	Routing Overhead	Detect False Misbehavior Report	Prevent Forged Acknowledgement	Solve Receiver Collisions Problem
4.	Detecting misbehaving nodes in MANETs	Enhanced Adaptive ACKnowledgement (EAACK) scheme which consists of three parts (i) Acknowledge (ACK) (ii) Secure ACKnowledgement(S-ACK) (iii) Misbehavior Report Authentication (MRA).	Same As AACK	Yeas	No	Yes
5.	Detecting Forged Acknowledgements in MANETs	Acknowledgement packets received in S-ACK phase of EAACK are digitally sign educing Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the SACK packet (EAACK2)	Same As AACK	Yes	Yes	Yes
6.	EAACK-A Secure Intrusion-Detection System for MANETs	The link between each node in the network is bi-directional, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.	Same As EAACK	Yes	Yes	Yes

5. Conclusion

Prevention of forged acknowledgement has always been a major threat to the security in MANETs. This survey paper, presented a survey on forged acknowledgement for MANETs. Most of the existing approaches are used to detect only the misbehavior links rather than the malicious nodes. Moreover, they fail to detect false misbehavior report in MANET. Prevent acknowledgement forging in MANETs is a challenge even though many approaches have been proposed against acknowledgement forging. Each scheme mentioned above except all EAACK techniques suffer from forged acknowledgement.

References

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, “EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE transactions on Industrial electronics, Vol. 60, No. 3 March 2013.

[2] S. Marti, T.J. Giuli, K. Lai, and M. Baker. “Mitigating Routing Misbehavior In Mobile Ad hoc Networks”. In the Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, pp. 255-265, Boston, Massachusetts, US, 2000.

[3] Balakrishnan, K.; Jing Deng; Varshney, V.K., 2005 “TWOACK: preventing selfishness in mobile ad hoc networks”, In Proceedings of Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp.2137-2142(March 2005).

[4] Liu K., Deng J., Varshney P.K. and Balakrishnan K., 2007, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs”. IEEE Transactions on Mobile Computing, May, 536-550.

[5] Liu K., Deng J., Varshney P.K. and Balakrishnan K., 2007, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs”. *IEEE Transactions on Mobile Computing*, May, 536-550.

[6] Kang, N., Shakshuki, E and Sheltami, T., 2010.” Detecting Misbehaving Nodes in MANETs”, In Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), ACM, pp. 216-222.

[7] Kang, N., Shakshuki E and Sheltami T. 2011 “Detecting Forged Acknowledgements in MANETs”, The 25thInternational Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society, Biopolis, Singapore.
Qasim M Alriyami, Eleana Asimakopoulou, NikBessis School of Computing and Mathematics, University of Derby, UK “A Survey of Intrusion Detection Systems for Mobile Ad-Hoc Networks”. 2014 International Conference on Intelligent Networking and Collaborative Systems.

[8] Shirina Samreen , G. Narasimha “An Efficient Approach for the Detection of Node Misbehaviour in a MANET based on Link Misbehaviou” 2013 3rd IEEE International Advance Computing Conference (IACC).

[9] Sivaranjani S, PG Scholar, Rajashree S, Assistant Professor “Secure Data Transfer In Manet Using Hybrid Cryptosystem” ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.

[10] Kejun Liu, Jing Deng, ,Pramod K. Varshney, , and Kashyap Balakrishnan “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs” International Conference on Computational Intelligence and Multimedia Applications 2007

[11] Vasantha. V, Dr. Manimegalai. D , K. R. Nagar, Kovilpatti, Tamilnadu “Mitigating Routing Misbehaviors using Subjective Trust Model in Mobile Ad hoc Networks” International Conference on Computational Intelligence and Multimedia Applications 2007.

[12] Swapna Taksande[1], Prof. Rajani Bhoomarker[2], Prof. Sameena Jafar[3] “Review Paper On Response Based Approaches For Detection Of Misbehaving Nodes In Manets” International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 3, Issue. 1, January 2014.

[13] A.Janani, A.Sivasubramanian,”Survey Of Packet Dropping Attack InManet” A.Janani et.al / Indian Journal of Computer Science and Engineering (IJCSE) Vol. 5 No.1 Feb-Mar 2014.

[14] K.Kirubani1, S.P.Anbukodi2 “A Secure Intrusion Detection System for Manets by using Cryptographic Algorithms” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. Vol. 3, Issue 3, March 2014.

[15] Sivaranjani S, Rajashree S "Secure Data Transfer In Manet Using Hybrid" ICICES2014.
[16] A. R.L.Rivest and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," 1978.
[17] R. Jhaveri, S. Patel, and D. Jinwala, "Dos attacks in mobile ad hoc net- works: A survey," in *Advanced Computing Communication Technologies (ACCT), 2012 Second International Conference on*, Jan 2012.
[18] M. Athulya and V. Sheeba, "Security in mobile ad-hoc networks," in Computing Communication Networking Technologies (ICCCNT), 2012 Third International Conference on, July 2012.
[19] P. Joshi, P. Nande, A. Pawar, P. Shinde, and R. Umbare, "Eaack- a secure intrusion detection and prevention system for manets," in *Pervasive Computing (ICPC), 2015 International Conference on*, Jan 2015