TRUST AWARE SECURE INTRUSION DETECTION IN MANET

[#1]M. Jegannath, [#2]Mr. P. Sivakumar
[#1]*PG Scholar, Department of Computer Science*
Manakula Vinayagar Institute of Technology
Pondicherry, India
[#2]*Associate Professor, Department of Information Technology,*
Manakula Vinayagar Institute of Technology
Pondicherry, India
[#1]jegannath1988@gmail.com,
[#2]ka_sivas@yahoo.co.in

***Abstract*— A mobile ad hoc network (MANET) is a self-configuring infra structure less network of mobile devices connected by wireless. 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. As the importance of MANET increases day to day, the vulnerability issues in MANET is important to be considered. The main issue concerned with MANET is partial dropping, ambiguous collisions, and collusion. A new intrusion-detection system named Robust Trust Aware Secure Intrusion Detection specially designed for MANETs. Compared to previous approaches, this technique demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.**

Keywords — Dynamic Source Routing, Intrusion Detection System, Misbehavior Report Authentication

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the security of the network. Since the impact would propagate in performing routing tasks, the risk aware model going to be implemented, takes risk into account to support more adaptive responses to routing attacks in MANET. This is achieved using Dempster-Shafer mathematical theory of evidence (D-S theory), which offers an alternative to traditional probability theory.

In MANET's each node may act as source or as a router. Nodes that cannot communicate directly depend on their neighbors in order to forward their messages to the appropriate destination. Applications of mobile ad hoc networks have increased requirements in order to ensure high quality of service for the provided services. Security in such infrastructure-less networks has been proven to be a challenging task. Many security threats arise against mobile ad hoc networks, as they are inherently vulnerable due to the way the build and preserve connectivity characteristics. The open medium presents the network with the first and most serious vulnerability. Unlike wired networks, ad hoc doesn't have any clear line of defense. Every node is vulnerable and the good performance of the network depends on every node or at least on every node participating in a path from the source to a given destination. The security threats based on partial dropping, collusion, ambiguous collisions is given a solution in order provide a strong wireless MANET application.

II. BACKGROUND

Many following research studies and implementations have proved that the Watchdog scheme is efficient. It fails to detect malicious misbehaviors with the presence of the following:

1) Ambiguous collisions
2) Receiver collisions
3) Limited transmission power
4) False misbehavior report
5) Collusion
6) Partial dropping

The AACK is a network layer acknowledgment-based scheme that may be considered as a combined system of TWOACK scheme and end-to-end acknowledgment scheme. It aims to solve the two problems of watchdog and improve the performance of TWOACK scheme by reducing the routing overhead while maintaining better performance. It is built on top of DSR routing protocol. The end to- end acknowledgment mechanism the AACK. Performing end-to-end acknowledgments reduces the routing overhead of the TWOACK scheme especially with paths more than two hops. As in the TWOACK scheme, our scheme reports misbehaving links rather than misbehaving nodes. Detecting misbehaving links instead of nodes is considered as a drawback for TWOACK because it gives the misbehaving node more chance to drop more packets.

Therefore, this shortcoming by doing a partial detection for malicious nodes. This is done by detecting the exact misbehaving node in case when the other end of the link is the destination node

EAACK scheme fails to detect malicious misbehaviors with the presence of the following:

1) Ambiguous collisions
2) Collusion
3) Partial dropping

III. Problem Definition

The EAACK, methods to over efficient packet dropping in Mobile ad hoc network (MANET) is a self-organizing, self-configuring confederation of wireless systems. MANET devices join and leave the network asynchronously at will, and there are no predefined clients or server. The dynamic topologies, mobile communications structure, decentralized control, and anonymity creates many challenges to the security of systems and network infrastructure in a MANET environment. Consequently, this extreme form of dynamic and distributed model requires a revaluation of conventional approaches to security enforcements. Associations between nodes are used to identify and isolate the malicious nodes. Simulation results show the effectiveness of our scheme compared with conventional scheme.

In MANET's each node may act as source or as a router. Nodes that cannot communicate directly depend on their neighbors in order to forward their messages to the appropriate destination. Applications of mobile ad hoc networks have increased requirements in order to ensure high quality of service for the provided services. Security in such infrastructure-less networks has been proven to be a challenging task. Many security threats arise against mobile ad hoc networks, as they are inherently vulnerable due to the way the build and preserve connectivity characteristics. The open medium presents the network with the first and most serious vulnerability. Unlike wired networks, ad hoc doesn't have any clear line of defense. Every node is vulnerable and the good performance of the network depends on every node or at least on every node participating in a path from the source to a given destination. So the security threats based on partial dropping, collusion, ambiguous collisions is given a solution in order provide a strong wireless MANET application.

Partial dropping: A node can circumvent the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehavior threshold. Although the watchdog will not detect this node as misbehaving, this node is forced to forward at the threshold bandwidth. In this way the watchdog serves to enforce this minimum bandwidth. For the watchdog to work properly it must know where a packet should be in two hops.

Ambiguous collision: The ambiguous collision problem prevents A from overhearing transmissions from B. As illustrated, a packet collision occur at A while it is listening for B to forward on a packet. A does not know if the collision was caused by forwarding on a packet as it should or if B never forwarded the packet and the collision was caused by other nodes in A's neighborhood. Because of this uncertainty, A should instead continue to watch B over a period of time.

Collusions

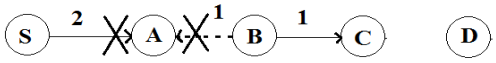

Figure 3.1 Collusion

If two nodes in a row collude, the Watchdog mechanism is observed to be failed at that case, it is explained as follows,

- Node A sends a packet to colluding Node B.
- Node B forwards the packet to other colluding Node C.
- Node C drops the packet and Node B does not report it.

Do not have two untrusted nodes in a row in a path.

It assumes that the nodes act by themselves.

IV. Scheme Description

A selective packet drop is a kind of denial of service where a malicious node attracts packets and drops them selectively without forwarding them to the destination. As an example consider the scenario in figure 4.1. Here node 1 is the source node and node 7 is the destination node. Nodes 2 to 6 acts as the intermediate nodes. Node 5 acts as a malicious node. When source wishes to transmit data packet, it first sends out RREQ packets to the neighboring nodes. The malicious nodes being part of the network also receives the RREQ. The source node transmits data packets after receiving the RREP from the destination. As node 5 is also the part of routing path will receive the data packets and drops some of them while forwarding others. This type of attack is very hard to detect as the malicious nodes pretend to act like a good node.

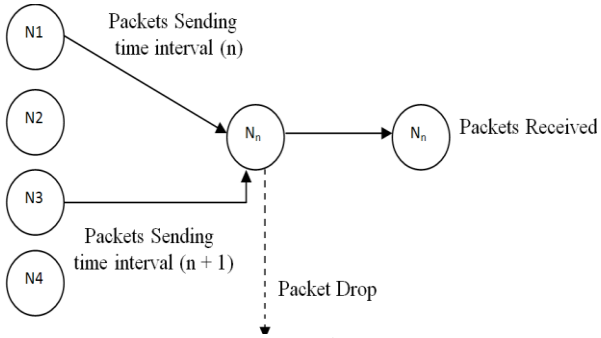

Figure 4.1 Structure flow diagram

The Association among the nodes and their neighboring nodes in to three types as below. In an adhoc network the Association between any node x and node y will be determined for the following defects

1) Partial Dropping

In an adhoc network the Association between any node x and node y will be determined as follows.

Unknown

- Node x have never sent/received any messages to/from node y
- Trust levels between them are very low.
- Probability of malicious behavior is very high.
- Newly arrived nodes are grouped in to this category.

Known

- Node x have sent/received some messages to/from node y
- Trust levels between them are neither low nor too high.
- Probability of malicious behavior is to be observed.

Companion

- Node x have sent/received plenty of messages to/from node y
- Trust levels between them are very high.
- Probability of malicious behavior is very less.

The source selects the shortest and the next shortest path. Whenever a neighboring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad hoc network are companions. Further the overheads due to the calculations of trust relationship are minimal compared to the CONFIDANT protocol. It will be slightly more than the normal DSR due to the invocation of the trust estimator whenever a data transfer is to be done through known or unknown.

2) Ambiguous Collision

This ambiguous collision can be overcome by minimizing the congestion that leads to collision. This congestion can reduced by optimizing the size of the contention window by parameters like source count and α in the network. If the contention window of a node is low, it results in collision. If the size of the contention window of a node is high then it results in a medium access delay. Thus minimizing congestion leads to reduce of collision and conserves energy.

3) Collusion

Evolution of wireless networking and mobile computing hardware have resulted in wide spread usage of mobile ad hoc networks in many distributed applications. The infrastructure less property and the easy deployment along with the self-organizing nature makes them useful for many applications like military applications and fast response to disasters. Despite it's applicability to multiple applications, the MANET cannot be considered as an alternative to a wired network and it demands a lot of research on security issues. In a MANET, communication can be established among nodes equipped with wireless transceivers without the usage of any routers. In other words, nodes themselves act as routers as well as source and they depend on each other for forwarding packets from a source to a destination. The main problem of communication in a MANET results from the inconsistency of the nodes to transmit the packet to some destination. This inconsistency results from a number of factors: Firstly, each node's transmission range is limited and nodes are mobile. Hence the dynamic nature of the network may cause a node which forwarded the data packets for some source/destination pair at some point of time, not being able to do so at a later point of time due to mobility which may affects transmission range. Secondly, the limited battery power of the nodes may effect it's packet forwarding behaviour.

Apart from these factors, the inherent characteristics of a MANET may cause the security of communication to be compromised easily. A node's capability of promiscuous overhearing of neighbourhood nodes within it's transmission range may raise issues for the confidentiality of data packets. Unlike wired networks, there is no clear line of defence in a MANET like a firewall or gateway and every node is vulnerable to an attack. The overall performance of the network depends upon every node since nodes have to collaborate for all network activities. The malicious adversaries usually exploit this feature of cooperative participation of nodes in the routing activity to launch attacks.

Hence we need to design security primitives for routing and also for detecting any adversaries in the network which launch various attacks. A packet drop attack is one of the attacks wherein the adversary simply drops the packets without forwarding. This may be due to it's selfishness to preserve battery power or it might have been compromised by an external attacker. To investigate the collaborative packet drop attack which is a serious threat to communication in MANET. Since MANETs are being used in a wide variety of applications involving data transmission, secure and robust data delivery to the destination has to be accomplished. A resource efficient and reactive approach to detect a packet drop attack is based on random audits on nodes for the behavioural proofs. It is resource efficient in the sense that it does not involve communication and computation overhead since it is triggered only when the destination senses a significant drop in the packet delivery ratio.

To develop a new mechanism for detecting colluding adversaries which together carry out a packet drop attacks. This system is a reactive and resource efficient approach for detecting a misbehaving node which carries out a packet drop attack individually. This approach fails in the presence of colluding adversaries. It is illustrated that a colluding adversarial model under which this approach fails for which another approach based on hash calculation on the received packets for node behavioural proofs has been proposed. But this approach requires the source node to share a secret key with each intermediate node. Two adversarial models involving colluding adversaries for which we have proposed detection mechanisms. The first adversarial model is the one wherein the colluding adversaries are two non-consecutive nodes separated by innocent intermediate nodes. The second one involves colluding adversaries

which are a set of consecutive nodes on the path from source to destination. Based on bloom filters used by proposed system as node behavioural proofs and does not require any secret to be shared between the source and the intermediate nodes.

V. CONCLUSION

Packet-dropping, Collusion and Ambiguous Collision attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named Trust Aware Secure Intrusion Detection System protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations.

REFERENCES

1. EAACK—A Secure Intrusion-DetectionSystem for MANETs Elhadi M. Shakshuki, *Senior Member, IEEE*, Nan Kang, and Tarek R. Sheltami, *Member, IEEE*.
2. K. Al Agha, M.-H.Bertin, T. Dang, A. Guitton, P. Minet, T. Val, andJ.-B.Viollet, "Which wireless technology for industrial wireless sensornetworks?The development of OCARI technol," *IEEE Trans. Ind. Electron.*,vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
3. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc NetworkSecurity," in *Lecture Notes in Electrical Engineering*, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.
4. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hocnetworks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana,India, 2012, pp. 535–541.
5. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in MobileAd Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.
6. L. Buttyan and J. P. Hubaux, *Security and Cooperation in WirelessNetworks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
7. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modelingand optimization of a solar energy harvester system for self-poweredwireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7,pp. 2759–2766, Jul. 2008.
8. 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.
9. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vectorrouting for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshopMobile Comput. Syst. Appl.*, 2002, pp. 3–13.
10. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routingprotocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*,Atlanta, GA, 2002, pp. 12–23.
11. G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routingprotocol—A review," *J. Comput.Sci.*, vol. 3, no. 8, pp. 574–582,2007.
12. D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wirelessnetworks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5,pp. 153–181.
13. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodesin MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10,2010, pp. 216–222.
14. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgementsin MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis,Singapore, Mar. 22–25, 2011, pp. 488–494.
15. K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile *ad-hoc* communicationsin AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323,2004.
16. J.-S. Lee, "A Petri net design of command filters for semiautonomousmobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4,pp. 1835–1841, Apr. 2008.
17. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "Anacknowledgment-based approach for the detection of routing misbehaviourin MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5,pp. 536–550, May 2007.

