INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

ADVANCED SECURE SYSTEM FOR MANET

K.Karthikeyani[1], A.Uma[2]

[1]PG Scholar,PGP College of Engineering and Technology,Namakkal
karthivsb@gmail.com
[2]Assistant Professor,PGP College of Engineering and Technology,Namakkal
kuttiumait@gmail.com
Address:198-1, vaiyapurinagar,ii crossr, Karur-639002,Tamilnadu, India
Mobile:9976548586,e-mail id: karthivsb@gmail.com

ABSTRACT

In the modernization world the usage of wireless network is more because of their scalability and mobility. MANET is most preferred by many applications because of its infra-structure less network model .The nodes in the network are self configurable. When two nodes comes in a range they communicate each other otherwise the communication is established through the neighbor nodes. This type of open medium of communication have high level of threats and attacks. To avoid this we deploy the intrusion-detection-system mechanisms to protect from attackers. By improving the security we can use our MANET system into various industrial applications and in emergency situations. In this paper, to propose and implement a new advanced secure system for MANET. This approach mainly focuses on the intrusion-detection and to improve the performance of the network. Mainly to use Enhanced Adaptive Acknowledgment method and different security methodologies to protect our network.

Keywords: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (AACK) (EAACK), Mobile Ad hoc Network (MANET).

1. INTRODUCTION

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.

An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may belogged for audit purposes and for later high-level analysis. Communication between two hosts using a network may be encrypted to maintain privacy. The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc Network(MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

By definition, Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, 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, attackers can easily compromise MANETs by inserting malicious or no cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

2. RELATED WORK

In a network or a system, any kind of unauthorized or unapproved activities are called intrusions. An Intrusion Detection System (IDS) is a collection of the tools, methods, and resources to help identify, assess, and report intrusions. Intrusion detection is typically one part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure intrusion is defined as: “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource” and intrusion prevention techniques2 (such as encryption, Authentication, access control, secure routing, etc.) are presented as the first line of defense against intrusions. However, as in any kind of security system, intrusions cannot be totally prevented. The intrusion and compromise of a node leads to confidential information such as security keys being revealed to the intruders. This results in the failure of the preventive security mechanism. Therefore, IDSs are designed to reveal intrusions, before they can disclose the secured system resources. IDSs are always considered as a second wall of defense from the security point of view. IDSs are cyberspace equivalent of the burglar alarms that are being used in physical security systems today]. As mentioned in, the expected operational requirement of IDSs is given as: “low false positive rate, calculated as the percentage of normalcy variations detected as anomalies, and high true positive rate, calculated as the percentage of anomalies detected”.

A. Requirements of IDSs

The IDS that is being designed should satisfy the following requirements:

*not introduce new weaknesses to the system, *need little system resources and should not degrade overall system performance by introducing overheads,

*run continuously and remain transparent to the system and the users,

*use standards to be cooperative and open,

*be reliable and minimize false positives and false negatives in the detection phase.

B. Classification of IDSs

*External intruder: An outsider using different means of attacks to reach the network.

*Internal intruder: A compromised node that used to be a member of the network

According to, insider attacks against ad-hoc networks use two types of nodes:

- Selfish node: Uses the network resources but does not cooperate, saving battery life for their own communications. It does not directly damage other nodes.

-Malicious node: Aims at damaging other nodes by causing network DoS by partitioning, while saving battery life is not a priority. An IDS can detect both external and internal intruders, but it should be noted that internal intruders are harder to detect. This is due to the fact that internal intruders have the necessary keying materials to neutralize any precautions taken by the authentication mechanisms.

Intrusion type: Intrusions in a network may happen in various ways:

Attempted break-in: An attempt to have an unauthorized access to the network.

Masquerade: An attacker uses a fake identity to gain unauthorized access to the network.

Penetration: The acquisition of unauthorized access to the network.

Leakage: An undesirable information flow from the network.

DoS: Blockage of the network resources (i.e., communication bandwidth) to the other users.

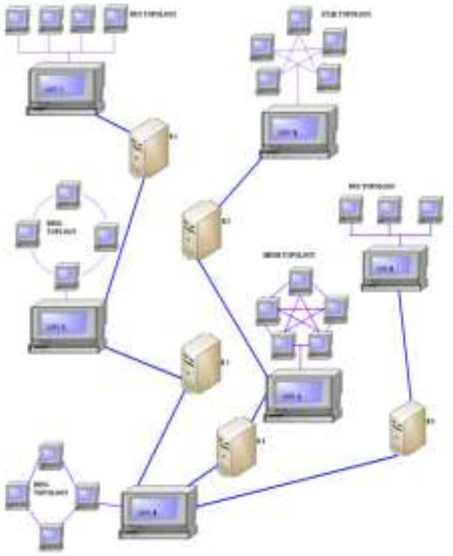
Malicious use: Deliberately harming the network resources.

IDSs may provide partial detection solution to those attacks. But of course, all system administrators would like to have a perfect IDS that would able to detect all of the intrusions listed above. Detection methodologies: IDSs are functionally categorized into three groups: anomaly based detection, misuse based detection, and specification based detection IDs are detected, depending on the level of the anomaly, either a local response is created or a global response is created among with the neighboring nodes. And communications pertaining to this global response should be assessed through secure communication links among the nodes. According to the authors, determining the features that would lead the modeling algorithm to detect anomalies with low percentage of false positive detection rates is a non-trivial.

The authors used two types of classifiers: Decision tree and Support Vector Machine. Updates of the routing tables are chosen as a trace data in three ways: percentage of the changed routes, percentage of changes in the sum of hops of all the routes, and the percentage of newly added routes. Trace analysis and anomaly detection are the two main methods for the IDS that are used by the authors. Data obtained from normal network routing operation is fed to the training algorithm to obtain reference values of the classifiers. Then deviations (correlate) from normal profile classifiers are used to determine the anomalies in the network routing.

3. PROPOSED METHODALOGY

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including DSA and RSA. 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, we adopt a digital signature in our proposed scheme named advanced secure system. MANET is a self-configuring infrastructure network of mobile devices connected by wireless network it equipped with both a wireless transmitter and a receiver that communicate each other bidirectional wireless either directly or indirectly. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi-hop. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. Due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks.



Architecture diagram

In particular, 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. 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 the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches.

4. IMPLEMENTATION MECHANISM

PROTOCOLS:

Table-Driven (or Proactive)

The nodes maintain a table of routes to every destination in the network, for this reason they periodically exchange messages. At all times the routes to all destinations are ready to use and as a consequence initial delays before sending data are small. Keeping routes to all destinations up-to-date, even if they are not used, is a disadvantage with regard to the usage of bandwidth and of network resources.

On-Demand (or Reactive)

These protocols were designed to overcome the wasted effort in maintaining unused routes. Routing information is acquired only when there is a need for it.

The needed routes are calculated on demand. This saves the overhead of maintaining unused routes at each node, but on the other hand the latency for sending data packets will considerably increase.

PROACTIVE:

DSDV (Destination-Sequence Distance Vector) DSDV has one routing table, each entry in the table contains: destination address, number of hops toward destination, next hop address. Routing table contains all the destinations that one node can communicate. When a source A communicates with a destination B, it looks up routing table for the entry which contains destination address as B. Next hop address C was taken from that entry. A then sends its packets to C and asks C to forward to B. C and other intermediate nodes will work in a similar way until the packets reach B. DSDV marks each entry by sequence number to distinguish between old and new route for preventing loop.

DSDV use two types of packet to transfer routing information: full dump and incremental packet. The first time two DSDV nodes meet, they exchange all of their available routing information in full dump packet. From that time, they only use incremental packets to notice about change in the routing table to reduce the packet size. Every node in DSDV has to send update routing information periodically. When two routes are discovered, route with larger sequence number will be chosen. If two routes have the same sequence number, route with smaller hop count to destination will be chosen. DSDV has advantages of simple routing table format, simple routing

Operation and guarantee loop-freedom. The disadvantages are (i) a large overhead caused by periodical update (ii) waste resource for finding all possible routes between each pair, but only one route is used.

REACTIVE:

On-demand Routing Protocols

In on-demand trend, routing information is only created to requested destination. Link is also monitored by periodical Hello messages. If a link in the path is broken, the source needs to rediscovery the path. On-demand strategy causes less overhead and easier to scalability. However, there is more delay because the path is not always ready. The following part will present AODV, DSR, TORA and ABR as Characteristic protocols of on-demand trend.

AODV Routing

Ad hoc on demand distance vector routing (AODV) is the combination of DSDV and DSR. In AODV, each node maintains one routing table. Each routing table entry contains:

Active neighbor list: a list of neighbor nodes that are actively using this route entry. Once the link in the entry is broken, neighbor nodes in this list will be informed.

Destination address

Next-hop address toward that destination

Number of hops to destination

Sequence number: for choosing route and prevent loop

Lifetime: time when that entry expires

Routing in AODV consists of two phases: Route Discovery and Route Maintenance. When a node wants to communicate with a destination, it looks up in the routing table. If the destination is found, node transmits data in the same way as in DSDV. If not, it start Route Discovery mechanism: Source node broadcast the Route Request packet to its neighbor nodes, which in turns rebroadcast this request to their neighbor nodes until finding possible way to the destination. When intermediate node receives a RREQ, it updates the route to previous node and checks whether it satisfies the two conditions: (i) there is an available entry which has the same destination with RREQ (ii) its sequence number is greater or equal to sequence number of RREQ. If no, it rebroadcast RREQ. If yes, it generates a RREP message to the source node. When RREP is routed back, node in the reverse path updates their routing table with the added next hop information. If a node receives a RREQ that it has seen before(checked by the sequence number), it discards the RREQ for preventing loop. If source node receives more than one RREP, the one with greater sequence number will be chosen. For two RREPs with the same sequence number, the one will less number of hops to destination will be chosen. When a route is found, it is maintained by Route Maintenance mechanism: Each node periodically send Hello packet to its neighbors for proving its availability. When Hello packet is not received from a node in a time, link to that node is considered to be broken. The node which does not receive Hello message will invalidate all of its related routes to the failed node and inform other neighbor using this node by Route Error packet. The source if still want to transmit data to the destination should restart Route Discovery to get a new path. AODV has advantages of decreasing the overhead control messages, low processing, quick adapt to net work topology change, more scalable up to 10000 mobile nodes.

However, the disadvantages are that AODV only accepts bi-directional link and has much delay when it initiates a route and repairs the broken.

DYNAMIC SOURCE ROUTING PROTOCOL

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. DSR was specifically designed for use in multi-hop wireless ad hoc networks. Ad-hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration. For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (On-Demand-Routing). In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the addresses of the intermediate nodes of the route in the packets. Compared to other reactive routing protocols like ABR or SSA.

DSR is beacon-less which means that there are no hello-messages used between the nodes to notify their neighbors about her presence. DSR was developed for MANETs with a small diameter between 5 and 10 hops and the nodes should only move around at a moderate speed.DSR is based on the Link-State-Algorithms which mean that each node is capable to save the best way to a destination. Also if a change appears in the network topology, then the whole network will get this information by flooding.

5. CONCLUSION

Firstly, to presented specific vulnerabilities of this new environment. Then surveyed the attacks exploit these vulnerabilities and, possible proactive and reactive solutions proposed in the literature. Attacks are classified into passive and active attacks .In this research paper, I have proposed a novel IDS named EAACK protocol specially de-signed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. To analyze the security threats an ad hoc net-work faces and present the security objectives that need to be achieved. On hand, the security-sensitive applications of ad hoc networks require a high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. The idiosyncrasy of ad hoc networks poses both challenges and opportunities for these mechanisms. This article focuses on how to secure routing and how to establish a secure key management semi in an ad hoc networking environment.

The article represents the first step of our research to analyze the security threats, understand the security requirements for ad hoc networks, and identify existing techniques, as well as propose new mechanisms to secure ad hoc networks. More work needs to be done to deploy these security mechanisms in an ad hoc network and to investigate the impact of utilize security mechanisms on network performance.

REFERENCES

[1] 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.
[2] 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.
[3] 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.

[4] 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.
[5] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, “Modeling 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] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
[8] G. Jayakumar and G. Gopinath, “Ad hoc mobile wireless networks rout-ing protocol—A review,” J. Comput. Sci., vol. 3, no. 8, pp. 574–582,2007.
[9] 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.
[10] 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.

A Brief Author Biography

K.Karthikeyani – Completed DECE in Periyar Centenary Girls Polytechnic, B.E(COMPUTER SCIENCE AND ENGINEERING) in P.G.P College of Engineering and Technology under Anna University Chennai, M.B.A(E-BUSINESS) in Annamalai University. Now pursuing M.E (COMPUTER SCIENCE AND ENGINEERING) in PGP College of Engineering and Technology under Anna University, Chennai. My research interests include Networks.

A.Uma – Completed B.E(COMPUTER SCIENCE AND ENGINEERING) in P.G.P College of Engineering and Technology under Anna University Chennai, M.E (COMPUTER SCIENCE AND ENGINEERING) in P.G.P College of Engineering Technology under Anna University Chennai. Working as Assistant Professor in PGP College of Engineering and Technology. My research interests include Peer to Peer Networks.