International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 1, January-February 2015 **ISSN 2278-6856**

Review on Improving Security Mechanism for MANET Using Adaptive IDS

Trupti G.Ghongade[1], Avinash P.Wadhe[2]

[1] ME Second Year Department of CSE, G.H.Raisoni College of Engg and Management, Amravati (MS),India

[2] MTech(CSE), G.H.Raisoni College of Engg and Management, Amravati(MS),India

Abstract

Mobile Ad hoc network has become one of the most wireless communication mechanisms. Mobile Ad-hoc Networks (MANETS) is a collection of wireless nodes without any infrastructure support, every single node works as both transmitter and receiver .Nodes communicates directly with each other when they are in a same communication range. The self-configuring ability of nodes in MANET makes them popular among vital mission applications like military use or emergency recovery. However the open medium allows MANET vulnerable to attacks. Because of MANET's distributed architecture and changing topology a traditional centralized monitoring system is no longer feasible in MANET .In this case detection should be focused as another part before an attacker can damage the structure of the system. So, this work presents various intrusion detection system named as TWOACK, AACK, ACK and Enhanced Adaptive Acknowledgement (EAACK).Enhanced intrusion detection system use digital signature technique to digitally sign packets before they are transmitted to ensure integrity and confidentiality.

Keywords: Mobile Ad hoc Network (MANET), Digital Signature, Enhanced Adaptive Acknowledgement (EAACK),IDS.

1.INTRODUCTION

Mobile Ad hoc Network (MANET) is a type of Wireless ad hoc network. Among all the contemporary wireless Networks MANET is one of the most and unique application. It is deployed in applications such as research and rescue, military and disaster recovery.

A Mobile Ad hoc Network is a collection of wireless mobile nodes that are capable of communicate with every other nodes without any fixed infrastructure. They communicate with each other via bidirectional wireless links either directly or indirectly and communication occurs within the transmission range due to limited resource of energy for each node. This means that two nodes cannot communicate with each other if

they are beyond the communication range of they are beyond the communication range of their own. In MANET pair of nodes exchange message either over a direct wireless links or over a sequence of wireless links including one or more intermediate nodes.

MANET is also capable of creating self- configuring and self-maintaining architecture without the need of any centralized infrastructure, often feasible in critical applications like military conflict, emergency services. These characteristics make MANET ready to be used in emergency circumstances where such centralized infrastructure is unavailable. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility.

However considering the fact that MANETS are very popular in critical mission applications and because of open medium and wide distribution of nodes make it vulnerable to various types of attacks, at all layers, including in particular the network layer, because the deksign of most MANET routing protocols assumes that there is no malicious intruder node in the network . So, network security plays an important role in MANET .Due to nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. Considering the fact that most routing protocols in MANET assume that every node in the network work cooperatively with other nodes, this assumption leaves the attackers with the opportunities to achieve significant on the network with just one or two compromised nodes. To address this drawback, IDS should be added to enhance the security level of MANET. If MANET can detect the attacker as soon as they enter the network it will be completely eliminate the potential damage if caused by compromised node at the first time.

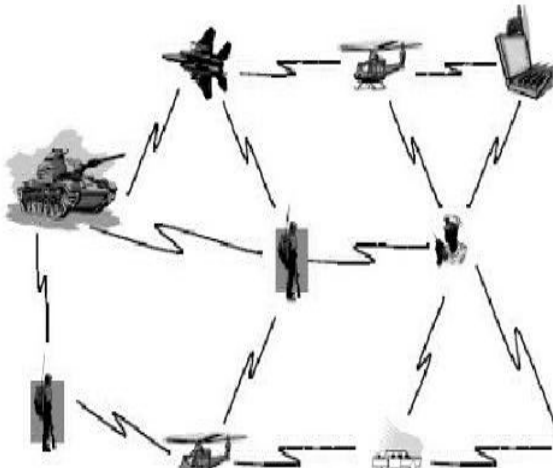

Figure 1 MANET Architecture

2.LITERATURE SURVEY

Intrusion detection system is defined as a technique to identify set of actions that attempt to compromise integrity, confidentiality and availability of source. The general function of IDS is to detect misbehavior in network. Providing security by detecting misbehaving nodes in network is an important research goal in MANET. The field is very important for research point of view. The review of work is as follows-

S. Marti, T. J. Giuli, K. Lai, and M. Baker [9] describes that most of the routing protocols in mobile ad hoc networks have limitations in transmission during communication. EacK2h node in MANET behaves co-operatively with each other to relay packets. This assumption gives opportunities to attackers to achieve significant impact on the network by inserting one or two non co-operating nodes or by compromising nodes. To address this issue IDS is added to enhanced security level of MANET. This paper introduced an intrusion detection system called watchdog system, consists of two parts namely watchdog and pathrater. Watchdog aims to improve the network throughput in the presence of malicious nodes.Pathrater helps to find that route that do not contain malicious node. Watchdog system contains a failure counter, which increased if he finds that its next node fail to forward a packets to the another node.

Y. Hu, A. Perrig, and D. Johnson [8] describes that an MNAET is a group of wireless mobile nodes, in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. These paper present attacks against routing in ad hoc networks, and present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

N. Nasser and Y. Chen [6] introduced a new intrusion detection system called ExWatchdog system to overcome the weakness of watchdog system. ExWatchdog is an improvement of traditional Watchdog system and its function is also of detecting intrusion from malicious nodes and reports that information to the response system, Routeguard. It aims to identify nodes that falsely report other nodes s misbehaving nodes. ExWatchdog system contains two parts: Watchdog and routeguard. Either in watchdog or routeguard, each node updates rating of nodes as it knows according to the information provided by any node in the network. A malicious node could partition the network by claiming that some nodes following it in the path are misbehaving nodes. ExWatchdog detection system is proposed to solve this problem.

K.Liu, J. Deng, P. K. Varshney, and K. Balakrishnan [5] outline a 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. It is used to detect some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. 2ACK scheme send two hop acknowledgment packets in the opposite direction of the routing path. It is a network-layer technique to detect misbehaving links rather than nodes and to mitigate their effects. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. 2ACK transmission takes place for every set of triplets along the route. Therefore, only the first router from the source will not serve as a 2ACK packet sender. The last router just before the destination and the destination will not serve as 2ACK receivers. To reduce additional routing overhead only a fraction of the received data packets are acknowledged in the 2ACK scheme. TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. Source send data packet to receiver. Receiver generates the 2ACK packet back to sender. Retrieval of 2ACK packet within a predefined time period indicates successful transmission otherwise both destination and intermediate nodes are reported as malicious.

N. Kang, E. Shakshuki, and T. Sheltami [4] describes that an ad hoc networks employ a decentralized unstructured networking model that relies on node cooperation for key network functionalities such as routing and medium access. This paper develop a model based on the Sequential Probability Ratio Test to characterize how nodes can differentiate between routes that include misbehaving nodes and routes that do not. An advantage of the model is that the number of observations required to evaluate a route need not be determined in advance, which suits well the dynamic nature of ad hoc networks. It then outline a centralized and a localized approach to detect misbehaving nodes on infected routes identified by the model. This evaluation shows that the localized approach is not only the better architectural choice for ad hoc networks but also results in a more accurate exposure of misbehaving nodes while incurring low false positives and low false negatives.

N.Kang, E. Shakshuki, and T. Sheltami [3] describes that MANET suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets transmitted during communication. This paper introduces an intrusion detection scheme with digital signature algorithm to provide secure transmission against false misbehavior report and partial dropping. This intrusion detection system assumes that communication link between nodes in

the network is bidirectional. Misbehaving nodes also lies in the network, behaving selfishly to preserve their own battery. It assumes misbehaving nodes are intermediate nodes, they are neither the source node nor the destination node. In routing stage they cooperate with other nodes but they drop the packets instead of forwarding to next node. After dropping the packets the misbehaving node generate a forge acknowledgement and sent it to source node in order to conceive the source node. When the source node sends out the data packet it registers the packet ID and sent time. After receiving packet, destination node needs to send acknowledgement packet back to the source node. Successful reception of acknowledgement packet at source node within a predefined time means transmission is completed and confirmed. Otherwise it will switch to the secure acknowledge mode. In this scheme, for every three consecutive nodes along the transmission route, the third node is required to send back an S-ACK packet back to the first node to confirm receiving the packet. In this system the third node is required to sign this S-ACK packet with its own digital signature. The intention of doing this is to prevent the second node from forging the S-ACK packet without forward the packet to the third node. When the first node receives this S-ACK packet, it verifies the third nodes digital signature with the predistributed public key. On the other hand, if no S-ACK packet is received within a predefined time period; the first node will report both second node and the third node as malicious. When the source node receives the malicious report, instead of trusting the report immediately and marks the nodes as malicious, it requires the source node to switch to MRA mode to confirm. The source node switches to MRA mode by sending out an MRA packet to the destination node via a different route. If such route does not exist in the cache, the source will find a new route. For extreme conditions when there are no alternative routes from source node to the destination node, this detection system, by default, accepts the misbehaving report.

In this paper R. Akbani, T. Korkmaz, and G. V. S. Raju [2] discuss security issues and their current solutions in the mobile ad hoc network. Owing to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. This paper first analyzes the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then it discusses the security criteria of the mobile ad hoc network and presents the main attack types that exist in it.

3. INTRUSION DETECTION SYSTEM FOR MANET

The basic conditions for intrusion detection are that there are intrinsic and notable characteristics of normal behavior that can be collected and analyzed and that it is possible to use those characteristics and behaviors to distinguish normal from abnormal behavior. Intrusion detection system has ability to detect an attack as soon as it starts its inappropriate activities in the network. So it would be possible to stop those activities before they cause any damage to the exchanged data between networks. Most traditional intrusion detection systems Watchdog mechanism was proposed by Marti et al. [10] along with Pathrater mechanism. First one is the intrusion detection system which is watchdog that identifies misbehaving nodes in MANET, aiming to improve network throughput with the presence of selfish or malicious nodes and other one is the response of intrusion detection system which is pathrater that helps the routing protocol to avoid these nodes. However, Watchdog mechanism's ability to detect malicious behavior is failed when one of the six situations occurs:1) ambiguous collision 2) receiver collision 3) limited transmission power 4) false misbehavior 5) collusion 6) partial dropping.

To solve these issues, many researchers proposed improved IDSs: TWOACK [5] is one of the most important contributions in intrusion detection mechanism.

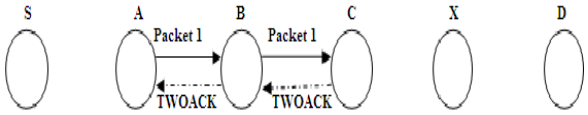

Figure 2 TWOACK Scheme

The idea is to let every three consecutive node to verify whether the sent packet has been received by the node that is two hops away from it. This is achieved by using acknowledgement packet called TWOACK. TWOACK scheme can be added into source routing protocols like DSR. TWOACK enhances watchdog by solving the problem of detecting misbehaving nodes in the presence of collisions and limited transmission power, but it is still vulnerable to false misbehavior attack. AACK [10] is another very important IDS specially designed for MANETs. It is a network layer acknowledgement-based scheme that can be considered as a combination of TWOACK and end-to-end acknowledgement scheme. By the introduction of adaptive scheme, AACK greatly reduce the network overhead when no misbehavior is detected as compared to TWOACK.

4. ENHANCED INTRUSION DETECTION SYSTEM FOR MANET

Enhanced intrusion detection system (EAACK) can be mainly divided into three parts ACK, S-ACK and MRA .The source node first searches for its local memory to see if there are any existing routes leading to the destination node [3]. If yes, data packets are sent via one of these routes. If not, it uses DSR to find a new routing path. These data packets contain a two bit header that indicates the type of packet. In this, general data packet has a header of "00", ACK packet is "01", S-ACK as "10" and MRA packet as "11".

When the source node sent out data packet, it registers the ID and sent time of packet. On the destination node, upon receiving a data packet, destination required sending back an ACK acknowledgement packet along the same route

but in a reverse order, which contains the ID of packet. If the source node successfully received this ACK packet within a predefined time, then transmission from source node to destination node is successful and confirmed. However, after a certain time out, if the source node does not receive the desired packet from the destination node, it will switches to S-ACK mode by sending out an S-ACK packet to the destination node along the same route.

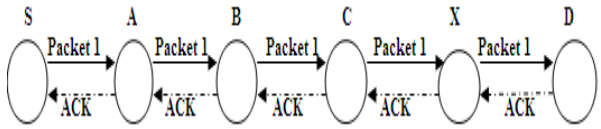

Figure 3 ACK Scheme

The S-ACK mode is an improved version of TWOACK [5] scheme. For every three consecutive nodes along the same transmission route, the third node is required to send back an S-ACK packet back to the first node to confirm receiving the packet. The third node is required to digitally sign this S-ACK packet with its own digital signature. The purpose of doing this is to avoid the second node from forging the S-ACK packet without forwarding the packet to the third node. When the first node receives this S-ACK packet, it verifies the third nodes signature with the pre-distributed public key. On the other hand, if no S-ACK packet is received within a predefined time period, the first node will report both second and the third node as malicious node [1]. Unlike TWOACK scheme, when the source node receives the malicious report, instead of trusting the report immediately and marks the nodes as malicious, enhanced intrusion detection system requires the source node to switch to MRA mode to confirm misbehavior report.

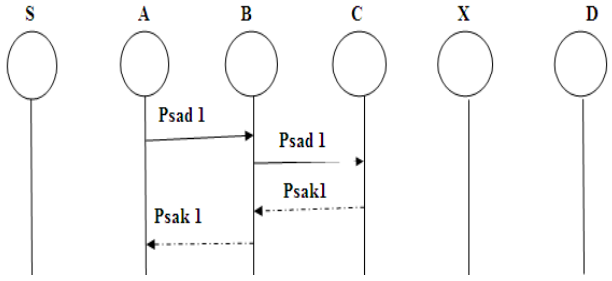

Figure 4 S-ACK Scheme

The source node switches to MRA mode by sending out an MRA packet to the destination node via a different route. If no such route exists in the cache, the source node initiates a new DSR route request to find a new route. The MRA packet contains the data packet ID. When destination node receives the MRA packet, it searches through its local knowledge base to find out whether the requested packet ID exists. If yes, then the data packet has been received and whoever sent the report is the misbehaving node. Otherwise, the misbehavior report is accepted and confirmed. For extreme conditions when there are no optional routes from source node to the destination node, enhanced intrusion detection system by default, accepts and confirms the misbehaving report.

5. SECURITY ANALYSIS

EAACK scheme in [1] is proposed to solve four of the six weaknesses of Watchdog mechanism, namely: ambiguous collisions, receiver collisions, limited transmission power and false misbehavior.

5.1 Ambiguous Collision

For ambiguous collisions, Node A may fail to overhear the transmission of node B, due to collisions from Packet 2 .A packet collision can occur at A, while it is listening for node B to forward on a packet to node C.

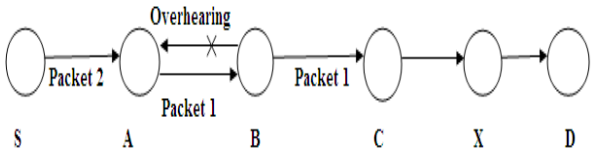

Figure 5 Ambiguous Collision

5.2 Receiver Collision

For receiver collisions, node A overhears that node B successfully forwarded Packet 1 to node C, but failed to detect that node C did not receive Packet 1 due to a collision with Packet 2.

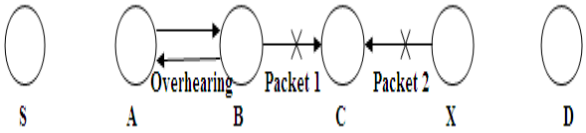

Figure 6 Receiver Collision

5.3 Limited Transmission Power

For limited transmission power, Node B is strong enough to be overheard by node C, but not strong enough to be received by node C because limited transmission power.

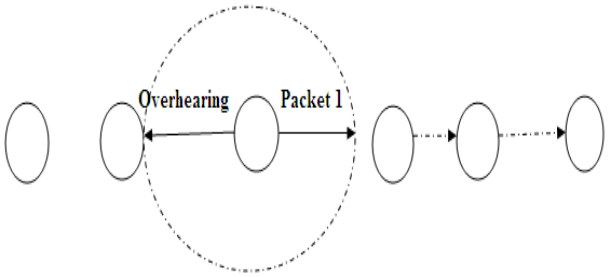

Figure 7 Limited Transmission Power

5.4 False Misbehavior Report

In false misbehavior report, node B successfully forward Packet 1 to node C, and node A also overhears that, node B forward that packet to node C , but still reports node B as misbehaving node. Due to the open medium of MANETs, attackers can easily capture one node and get this misbehaving report attack.

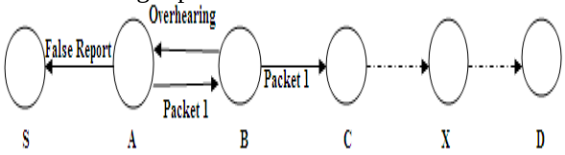

Figure 8 False Misbehavior Report

Traditional intrusion detection systems TWOACK and AACK solve two of these four weaknesses namely receive collision and limited transmission power. However both of them are vulnerable to false misbehavior attack. EAACK scheme in [1] solve this four potential attacks to watchdog with the introduction of digital signature. In this scheme nodes are required to digitally sign important packets so that infected packets can be detected.

6. CONCLUSION

Mobile ad hoc networks are an increasingly promising area of research with many practical applications in military and civilian communication. Because of dynamically changing topology, infrastructure less architecture MANETS is vulnerable to various types of attacks. To address these attacks, prevention mechanism alone are not enough to manage the secure mobile network, in such case detection should be focused as another part before attacker can damage the system.

In this paper different Intrusion detection systems are reviewed namely Watchdog, TWOACK, AACK and EAACK. Watchdog scheme identifies the misbehaving nodes in MANET and aiming to improve the throughput in presence of malicious nodes. But it fails to detect malicious misbehavior in presence of receiver collision, limited transmission power, false misbehavior attack etc. TWOACK and AACK solve receiver collision and limited transmission power but they again fail to detect nodes in presence of false misbehavior attack.

New enhanced intrusion detection system EAACK is better than Watchdog, TWOACK and AACK scheme. It solves all of these problems of receiver collision, limited transmission power and false misbehavior problem in traditional IDS.

In addition to prevent attackers from forging acknowledgement packets digital signature scheme is incorporated into the enhanced intrusion detection system (EAACK).

References

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs", IEEE Transactions on Industrial Electronics. Vol.60, no.3,MARCH, 2013.

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

[3] 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.

[4] 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.

[5] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Transaction in Mobile Computing., vol. 6, no. 5, pp. 536–550, May 2007.

[6] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Communication., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159

[7] 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 Computing. Syst. Appl, 2002, pp. 3–13.

[8] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23

[9] 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 Computing . Netw., Boston, MA, 2000, pp. 255–265.

AUTHOR

Trupti Ghongade did B.E in Information Technology from Amravati University, Dr.Sau Kamaltai Gawai College of Engg.& Technology, Amravati in 2012.She is pursuing for ME CSE from G.H. Raisoni, Amravati. Her research interest includes Networking,Network Security.

Prof. Avinash P. Wadhe did B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU Amravati University. His research interest include Network Security, Digital forensics .He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference. Currently he completed his diploma in cyber forensics.