Mobile Adhoc Network Security Issues and Proposed Solutions

Sahasrangshu Pal Choudhury

Abstract— *Mobile Ad Hoc Network (MANET) is a cluster of communication nodes that can communicate with each other without any requirement of fixed infrastructure or designated routing links. The nodes in MANET can do self-discovery of other nodes to communicate between each other and form a dynamic network. . This flexibility makes them attractive for many applications such as military applications, where the network topology may change rapidly to reflect a force's operational movements, and disaster recovery operations, where the existing/fixed infrastructure may be nonoperational. The dynamic features of MANET bring this technology with a great opportunity bundled with severe challenges. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks This paper would describe most significant security issues and its trends, current research pertaining to detection and protection of MANET security vulnerabilities.*

Index Terms— AODV, Attacks, Intrustion, Mobile Communication, MANET, Routing, Vulnerability

1. Introduction

Unlike the conventional dedicated nodes to carry packets for routing and forwarding in MANET the nodes collaboratively perform the task of routing and network management. They use multi-hop communications with each other based on the range of their radio signals wirelessly (Sevil, ,et al., 2011) . The node that want to communicate to other nodes but are not within their radio signal uses an intermediate node to relay the message as a router to the end node. Due to this flexibility nodes can be mobile, register and deregister from the network created often this result in frequent route update and change of network topology (Sevil, et al., 2011). A node can be any device like a laptop, pda, smart phones which has the ability to communicate with each other(Datta & Marchang, 2012). Proposals are there for many kinds of routing protocols to suit different network needs however, most of them does not consider security vulnerabilities. AODV (Ad-hoc On-demand Distance Vector) is the most popular of all the protocols as its reactive and discovers route on demand (Sevil ,et al., 2011). "It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within ad hoc network" (Perkins, 2003 cited in Sevil, et al., 2011, p.130) . However, these between node cooperation based routing protocols are vulnerable to all types of attacks.

The lack of centralized node, dynamic routing change and the existence of highly constraint node presents the security challenges which would be explained in subsequently (Sevil ,et al.,2011).

2. Attack Types

The security attacks can generally be distinguished into two types.

Active attacks: As per (Misra & Goswami, 2011) in active attack, "the attacker gets access to the transmission channel and the transmission technique, so that he can change the data or transmit his own data in a camouflaged manner". These kind of attacks creates unauthorized state change of the network and attackers are usually a user or nodes with authorization to operate within the network (Sevil ,et al., 2011). According to (Sevil ,et al., 2011) active attacks can be grouped as dropping, modification, fabrication, and timing attacks. The major category of active attacks are (Datta & Marchang , 2012) :

Attacks by dropping packets, attacks using modification of protocol messages fields, attacks using impersonation, attacks using fabrication and Wormhole attacks

Passive attacks: In a passive attack, the attacker sniffs the network traffic or collects various information data from it, but the data are not manipulated they are more difficult to detect and counter (Misra & Goswami , 2011). Since in passive attack the attacker only monitors the network they normally do not relay data within network to damage the communication (Sevil ,et al., 2011). For an instance, the malicious passive node can eavesdrop on data passed through a specific node and analyses the behavior of the node which is crucial for routing and then may try to switch from passive to active to attack the traffic and the node (Datta & Marchang , 2012).

- *Sahasrangshu Pal Choudhury is currently pursuing masters degree program in Information Technology in Anglia Ruskin University, UK, PH-+255778953348. E-mail: sahasrangshu.choudhury@student.anglia.ac.uk*

3. Security Vulnerabilities

Attackers in MANET can be either an insider or outsider and the attack also varies depending on the network layer (Gokhale ,et al., 2011)tentative types of attacks are various layers are as follows:

Layer	Types of Attacks
Application	Data corruption, viruses and worms
Transport	TCP/UDP SYN flood
Network	Hello flood, blackhole
DataLink	Monitoring, traffic analysis
Physical layer	Eavesdropping, active interference

The above table does not restrict the type of attacks and not limited to this few. However, in the scope of this paper due to restriction of word count discussion will be limited to few most significant attacks and how are they organized. Subsequently this paper would define researches that are being conducted in the field of preventions of those attacks.

As per (Datta & Marchang , 2012) , (Gokhale ,et al., 2011)in **Blackhole** Attack a malicious node will broadcast its willing to participate in the network. The node will at beginning analyze the routing protocol mostly using eavesdropping information of the network traffic. The node will normally announce during route discovery that it knows the accurate path to the target nodes. Hence, this attack is not against route discovery packets but done with an intention of dropping all types of forwarding packets like control or data. This attack is conducted in both reactive and proactive routing path selection protocols. The network cannot determine an alternate route when such situation occurs as the malicious node (black hole) does not send any notification of forwarding packet failure to the originating node.

Unlike black hole, (Datta & Marchang , 2012)in **GreyHole** attacks the malicious attacker is selective in dropping packets so it determines forwarding routing packets and dropping data packets or vice versa. However, the decision of packet dropping pattern is related to the intention of the attacker. Nodes who implement routing topology selectively drop the packets and often found difficult to detect and also depending on drop rate and data dropped detection is a big challenge. It was also noted that sometimes overloaded nodes which drops packets are accidentally identified as Grey Hole attackers.

In **Wormhole** attack (Datta & Marchang , 2012) , (Sevil ,et al., 2011)and (Gokhale ,et al., 2011) the attacker tunnels the packet from one location to other and relays it from that location onwards and is performed in collusion of two or more nodes. Reactive protocols like DSR and AODV are more vulnerable as the attacker would tunnel every REQUEST packet to the target destination node directly. As result the neighboring nodes hearing this REQUEST would follow normal protocol and will rebroadcast the REQUEST packet and would also discard further REQUEST packets for route discovery hence the only wormhole routes are imitated as the only route alive in the network. Hence, all future packets from all nodes are routed to the same route and the attacker can launch now any sorts of attacks. A wormhole attack is one of the most sophisticated and severe attacks in MANETs.

The protocol vulnerability is also exploited by attackers at various stage of protocol handshaking within the network; this causes the attacker to have full control over the transport and network layer and can also cause DoS (Denial of Service) attacks. According to (Datta & Marchang , 2012) and (Garg, 2009) Attacks using modification of protocol message by getting access to the message applying **Eavesdropping** method. The significant ones are :

Remote Redirection using False Sequence number: (Datta & Marchang , 2012)AODV protocol assigns monotonically increased sequence number to routes towards a destination node. The case the malicious node would causes a redirection of network traffic and a DoS attack by altering control message fields and may also divert traffic through itself by advertising a route to another node by increasing the authenticated value of des destination_sequence_num field of the control messaging protocol (Garg ,2009).

Modified Hop-Count and Source Route: The route length of ADOV protocol is represented in the messages by the hop-count field. This hop-count determines the shortest path of the route. By broadcasting a shortest route (very low hop count) to a destination node, a malicious node can succeed in re-routing all the packets to a particular destination through itself. On the other hand malicious node can also set the Hop_count to 0. The DSR protocol explicitly states routes in the data packet which is known as source route. DoS attack can be launched by an attacker by modifying the packet header to create loop.

DoS attacks can be caused in MANET in various ways at various network levels like Network and Transport layers etc. MANET nodes are operating on Battery and power management is an issue of research for various scholars. However, (Sevil ,et al., 2011) and (Fadlullah ,et al., 2011) has mentioned attackers knowing the fact that such nodes has limited power creates **"sleep deprivation torture"** attack which in technical term attacker keeps who is active keeps on rushing packets to nodes till all its battery power are exhausted or (Stajano, 1999 et al cited in Sevil ,et al., 2011, p.135)is the most powerful of the **DoS attacks** and also causes CPU exhaustions. A proactive protocol of MANET normally updates the routing information periodically in the routing table before utilizing the route here an attacker will flood the network during Route Discovery by broadcasting many Route-request messages causing the victims routing table overflow as such restricting that node for new route discovery (Sevil ,et al., 2011).

Through this section the security vulnerabilities that MANET protocol possesses are mentioned and it clarified how the existing design of ADOV is being exploited by the attackers.

4. Security Solutions

There are two approach in which research are being conducted to secure MANET; Proactive and Reactive solutions. While Proactive is mean for Prevention, Reactive is meant for Detection and react (Rai & Singh, 2010; Das ,et al., 2012).

A. Proactive:-In this approach research has been conducted to mitigate security vulnerabilities through secured protocol communications and the use cryptographic technique.

B. Reactive: Here security is mitigated through reaction by implementing techniques to detect intrusions.

To secure the protocol and to build proactive measures according to (von Mulert ,et al., 2012) various extensions to secure AODV have been researched by scholars, like Secure AODV (SAODV) (Guerrero-Zapata, 2002), ARAN (Sanzgiri ,et al., 2002), SEAR (Li ,et al.,2008) and SEAODV (Mohammadizadeh ,et al.,2009). Following some of the protocol would be discussed along with their limitations.

SAODV secures manipulation of the AODV routing message by applying asymmetric cryptography the scope is not to provide confidentiality or integrity or authenticity of the data packet (von Mulert ,et al., 2012). SAODV use two cryptographic mechanisms, viz., digital signatures and hash chains (von Mulert ,et al., 2012) and it requires circulation of public keys and private keys and each node is able to verify the association of node based on public key of that node and assumes and existence of decentralized key management system(Datta & Marchang 2012). The ADOC message transmits the signature extension which contains hash chain and signature with following fields Type, Hash Function, Length, Top Hash, Signature, Max Hop Count, and Hash (Datta & Marchang , 2012). Digital signatures are used to protect the integrity of the nonmutable data in RREQ and RREP messages (Datta & Marchang , 2012). This prevents impersonation of the source nodes sending RREQ and destinations sending RREP (von Mulert ,et al., 2012). Authentication of RREQ and RREP mutable hop counts are controlled through hash chains as each nodes whether intermediate or destination which receives the message increment the hop count its signature is added to the hash chain as result preventing any node from decrementing the hop count. A (Datta & Marchang , 2012) node which receives a RREP, would verify the signature before creating or changing a route to that host and RERR message are all signed by the nodes to prevent tampering or impersonation also the protocol restricts the nodes to update Destination Sequence Number (DSN) from RERR or RREP preventing attacks that manipulate DSN (von Mulert ,et al., 2012; Datta ,et al., 2012). However, as its evidential that SAODV are vulnerable to insider attacks and can mitigate is limited to attacks which are caused by impersonation or manipulation of protocol routing messages and is not suitable for military application (Guerrero-Zapata, 2003 cited in von Mulert ,et al., 2012, p.1250).

Similar to SAODV the goal of other cryptographic protocols is to mitigate the risk of attacks conducted by modifying the mutable fields of the transmitted packets and also to ensure that transmitted packets are verified within the legitimate nodes. However, each of these protocols creates computational overheads to create the cryptographic techniques. Unlike SAODV Authenticated Routing for Ad Hoc Networks(ARAN) uses hop-by-hop and end-to-end authentication in Route Discovery Packets (RDPs, functionally similar to RREQs) (Sanzgiri ,et al., 2002 cited in von Mulert ,et al., 2012, p.1251). ARAN(Datta & Marchang, 2012) uses cryptographic certificates to prevent attacks aimed at disrupting the correct route discovery from source to destination. The RDP is signed by initiator node and unlike RREQs of SADOV in ARAN each node signs and authenticates the RDP, each intermediate node authenticates and removes the signature and signs the RDP before rebroadcasting it and destination node sends and REP (Reply Packet) in same route RDP broadcast was received, this allows each node maintains fresh certificates and end to end authentication is ensured from attacks like replay and route loop attacks (von Mulert ,et al., 2012). The RDP broadcast packet includes packet type identifier, the IP address of the destination, Certificate of the Initiating node and nonce , all Signed with the private key of the initiating node the nonce is to identify the RDP coming from and each time the initiator does the route discovery it increases the nonce monotonically(Datta & Marchang , 2012) and there is no mutable field in RDP (von Mulert ,et al., 2012).ARAN is computationally expensive security measure and still cannot prevent an unauthenticated node to enter the network route who can replay an unaltered RDP packet and the related REP(von Mulert ,et al., 2012).

The SEAR(Secure Efficient Ad hoc Routing)protocol, which is a secure extension of AODV builds a one-way hash function to create a set of hash values known as authenticators which is associated with each node(Li ,et al., 2008 cited in von Mulert ,et al., 2012, p.1250) to ensure authenticity of routing control message. A malicious node in SAODV may broadcast RREQ without increasing the hop count however SEAR prevents the same by encoding the node's identity into the hash values to create a hash tree (von Mulert ,et al., 2012). Broadcast authentication scheme TESLA (Timed Efficient Stream Loss-Tolerant Authentication) protects the route error message and SEAR secures AODV protocol by securing both sequence numbering and hop counts simultaneously and it requires asymmetric cryptography only in bootstrap phase ; hence, SEAR provides comprehensive solution with minimum overhead (Li ,et al., 2008)

Apart from the proactive cryptographic proposals a research is also evident on reactive measures like Intrusion Detection Systems (IDS) integrated within the nodes to detect and black list the intruder (von Mulert ,et al., 2012). The main functional module of IDS are data collection, detection and response where the data collection is responsible for collection and preprocessing data and transferring them in a common format in a data storage and then sending the data to the detection module Sen & Clark(2008 cited in Amiri ,et al., 2014, p.455). In broad category intrusion detection has been classified into 1. Signature Based Detection where knowledge about the signature is incorporated in the detection system and 2. Anomaly based intrusion detection system unlike Signature based it tries to apply logics to find abnormal network pattern behavior (Datta & Marchang , 2012). The Signature-based detection has an inherit weakness due to which new attacks cannot be detected as the signatures not yet incorporated in the IDS will go undetected and anomaly based detection also creates false alarms (Datta & Marchang , 2012). According to (Datta & Marchang , 2012)IDS can also be classified based on the data it uses for analysis and detection ; Host based IDS uses data collected from the host its checking like OS and Application Logs and the other kid of IDS collects data from the network traffic for analysis. Broadly (Amiri ,et al., 2014)the IDS architecture can be classified into three models 1. Stand-alone in which all nodes performs IDS on its own, 2. Cooperative model is where IDS of each node performs global active or passive decision making jointly by sharing intrusion detection information and last 3. Hierarchal in this model networks are divided in clusters and each cluster head node are responsible for detection of intrusion within that cluster, this architecture is considered to be effective on constraint resources but due to high mobility architecture of MANET establishing a cluster and cluster head is difficult and complex. However, like many existing security systems for wireless network like IDS are ineffective for many envisaged MANET network deployments. Researcher are working for last decade on developing new security solutions applicable to MANET(Sevil ,et al., 2011). Tseng ,et al. (2003 cited in von Mulert et al., 2012, p.1252) and Sevil et al. (2011) proposed that, neighbouring nodes can monitor the request and response flow by using a finite state machine (FSM) with a tree like structure of forwarding table during discovery phase and which can allow for network data analysis and create reputation bases system where neighbouring nodes assigns trust levels to each other by monitoring each other's RREP and RREQ messages. Using danger theory intrusion algorithm the researcher (Abdelhaq, et al., 2011 cited in Amiri ,et al., 2014, p.456) proposed dendritic cell algorithm (DCA) to detect sleep deprivation attack over MANET it follows Standalone architecture. Markov Chain based method within Cooperative architecture is proposed by Bo Sun at el. (2006 cited in Amiri ,et al., 2014, p.456) to develop a Zone based intrusion detection system to detect route disruption attack.

Mitrokotsa at el. (2007 cited in Amiri ,et al., 2014, p.458) proposed Neural network based classification algorithm which can be used to detect Blackhole, Forging, Packet-dropping and Flooding attack within Hierarchical Architecture. Hierarchical architecture based solution was also proposed by H. Otrok at el., (2008 cited in Amiri ,et al., 2014, p.457) to apply game theory based algorithms to detect Selfish attack. Barani & Abadi (2012 cited in Amiri ,et al., 2014, p.457) has developed "BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative Selection Algorithms" to detect Wormhole, Rushing and Flooding Attacks in Standalone architecture. Another technique for Intrusion Resistant Ad-hoc Routing Algorithms (TIARA) which applies the techniques for mitigating gratuitous data flows which includes Flow Based Route Access Control (FRAC) which behaves like a distributed firewall to mitigate depletion attacks where each nodes maintains a list of allowed flows through a defined access control list as such the protocol is modified to index the routing table with an identifier which is latter utlised for routing (von Mulert ,et al., 2012).

Determining whether the Cryptographic proactive method or IDS based Reactive method is a better solution for MANET security is not part of the scope of this paper however; merging both the measure can measurably bring more prudent mitigations to safeguard MANET vulnerabilities.

5. Future Research

Future work has several challenges as MANET is still evolving and securing ad-hoc network does not have any well-defined comprehensive solution in place. The main concern is that the mobile devices are battery powered and has limited storage and computational resources (Datta & Marchang , 2012). All the proposed methods/algorithm and techniques mentioned in this paper has power and processing overhead on the nodes. Hence, research in the field of hardware and resource efficiency of the node as well as algorithms which consume lesser resources are required to make the MANET security robust in nature(Datta & Marchang , 2012). On securing protocols researchers must work on a holistic approach to find solutions for comprehensive vulnerabilities covering from signal interception and jamming to sophisticated attacks conducted by authenticated nodes (von Mulert ,et al., 2012). Moreover, such approach to include all models of known attacks and vulnerabilities would help researchers to design a more comprehensive solution rather than attack specific solutions (Datta & Marchang , 2012). Research to utilize AODV's feature to find multiple and shortest routes should be utilized to design solutions or algorithm to support the redundancy of routing where one route is infested with attacks like DoS or Link Failure(von Mulert ,et al., 2012) . Research in the field of optimizing bandwidth allocation (RREQ rate limits) in a MANET with limited resources during resource depletion attacks is essentially required as well (Misra & Goswami , 2011). Research to develop security protocol and IDS that supports cooperation and communication between nodes and the concept of self-healing community where after identification of blacklisted node traffic is instantly re-routed through other path is another area that needs to be explored by researcher as it would be dynamic and robust security solution for MANET (von Mulert ,et al., 2012). Key management and hashing scheme is another area where research can be elaborated by developing schemes considering channel utilization and node storage capacity. Most of the Key management techniques have been proved mathematically or by simulators however, practical application and testing its robustness on various attacking schemes can be verified (Misra & Goswami , 2011).

There are no single ways through which MANET can be made secured hence, research on encrypted protocol, intrusion detection and access control violation should be combined to produce a future of a more secured MANET which handle large quantum of active and passive attacks.

6. Conclusion

In this paper major security issues of MANET are identified and their pattern, prospect and impact are being discussed in detailed. Most of the standard security attacks that are persisting in wireline network are also present in MANET . It was also significant to note that how the dynamic topology, resource constraint (bandwidth and battery) and lack of central protocol management increased the quantum of attacks and its impact on MANET. MANET routing was introduced in brief along with most popular ADOV protocol was explained. Introduction to type of attacks like Active and Passive and their mode of operandi, their subsequent significant security vulnerabilities and type of scenarios at various layers of network was discussed. Most of attacks discussed were active routing based attacks that were classified as fabrication, modification, dropping and incorrect routing based attacks.

ADOV and its incapability to prevent malicious attacks and how various SADOV protocol cryptographic proactive methods can be useful were examined and their limitation was understood. This paper also discussed various well-known intrusion methods and presented and compared reactive security prevention methods defined under Intrusion Detection Systems to handle various kinds of security vulnerability scenarios. Furthermore, key and hashing techniques and their limitation in MANET due infrastructural and topological constraint of the nodes were understood. Most significantly emphasis of resource limitation and complexity of these reactive and proactive security algorithms and their overhead were understood.

Having discussed various paradigm of MANET security in this paper I have significantly developed a comprehensive understanding of MANET topology, security issues and various methods of attack preventions. It was also pertinent to note that conventional security techniques were not directly efficient in MANET security vulnerability prevention. Additionally, in this paper after discussing prevention methods, significant future research trends were discussed which would allow a secured MANET based communication network to be used more practically within commercial and military use.

References

Amiri, E. et al., 2014. Intrusion Detection Systems in MANET: A Review. Procedia - Social and Behavioral Sciences, 129, pp.453–459. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1877042814028821 [Accessed June 4, 2014].

Datta, R. & Marchang, N., 2012. Handbook on Securing Cyber-Physical Critical Infrastructure□: Foundations and Challenges Chapter 7□: Security for Mobile Ad Hoc Ne tworks. In Elsevier Science and Technology Books, Inc.., pp. 147–190.

Fadlullah, Z.M., Taleb, T. & Schöller, M., 2011. Combating against Security Attacks against Mobile Ad Hoc Networks (MANETs). In A.-S. K. Pathan, ed. Security of Self-Organizing Networks. Florida: Auerbach Publications Taylor & Francis Group, pp. 173–194.

Garg, N., 2009. MANET Security Issues. IJCSNS International Journal of Computer Science and Network Security, 9(8), pp.241–246.

Gokhale, V., Ghosh, S.K. & Gupta, A., 2011. Classification of Attacks on Wireless Mobile Ad Hoc Networks. In A.-S. K. Pathan, ed. Security of Self-Organizing Networks. Florida: Auerbach Publications Taylor & Francis Group, pp. 195–225.

Kumar, A.B.R., Reddy, L.C. & Hiremath, P.S., 2008. MOBILE AD HOC NETWORKS□: ISSUES , RESEARCH TRENDS AND EXPERIMENTS. IETECH Journal of Communication Techniques, 2(2), pp.57–63.

Li, Q. et al., 2008. SEAR□: A Secure Efficient Ad Hoc On D emand Routing Protocol for Wireless Networks. ACM symposium on information computer and communications security, pp.201–4. Available at: http://users.crhc.illinois.edu/yihchun/pubs/asiaccs08.pdf.

Misra, S. & Goswami, S., 2011. Key Management in Mobile Ad Hoc Networks. In A.-S. K. Pathan, ed. Security of Self-Organizing Networks. Florida: Auerbach Publications Taylor & Francis Group, pp. 148–170.

Von Mulert, J., Welch, I. & Seah, W.K.G., 2012. Security threats and solutions in MANETs: A case study using AODV and SAODV. Journal of Network and Computer Applications, 35(4), pp.1249–1259. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1084804512000331 [Accessed July 3, 2014].

Rai, P. & Singh, S., 2010. A Review of " MANET " s Security Aspects and Challenges '. IJCA Special Issue on "Mobile Ad-Hoc Network", MANETs, pp.162–166.

Sevil, S., Clark, J.A. & Tapiador, J.E., 2011. Security Threats in Mobile Ad Hoc Networks. In A.-S. K. Pathan, ed. Security of Self-Organizing Networks. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Florida: Auerbach Publications Taylor & Francis Group, pp. 127–145.