A Survey of Various Risk Mitigating Techniques in MANET Environment

P.J Sweetlin Subha[1], Jeban Chandir Moses[2]

[1]Post Graduate student, Department of Computer Science and Engineering, Karunya University, India
[2]Lecturer, Department of Computer Science and Engineering, Karunya University, India

Abstract- Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. MANET has the dynamic infrastructure hence it is highly vulnerable to attacks. Several attacks are possible in MANET networks and among them routing attack could cause the worst damage. There are several solutions available for mitigating the routing attacks based on the intrusion response techniques but most of them isolate the malicious node only based on the binary decisions taken for severity in attacks. This will cause additional damage to the network. Risk mitigating techniques is one of the important factor in MANET environment. This paper surveyed various risk mitigating techniques and compare their various parameters. Existing techniques does not consider the Risk in taking countermeasures. Therefore there is a need to implement the new risk mitigating technique that consider the risk of both routing attacks and their countermeasures.

Index Terms- MANET, Intrusion response, Risk Aware.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring and infrastructure less network of mobile devices that are connected by wireless. Each device in a MANET hence freely move independently in any direction, and each device will therefore change its links to other devices frequently. Each device must forward the traffic unrelated to its own use, and hence act as a router. Mobile Ad hoc Networks (MANET) are used to set up wireless communication in the improvised environments without a predefined infrastructure and centralized administration. Therefore, MANET is normally deployed in adverse and the hostile environments where the central authority point is not necessary. Another outstanding characteristic of MANET is its dynamic nature of network topology which would be hence frequently changed due to the unpredictable mobility of the nodes. Furthermore, each mobile node in the MANET plays a router role while transmitting required data over the network. Hence, any compromised nodes could cause significant damage to the functionality and security of its network since the impact of the malicious node would propagate in performing routing tasks.

Intrusion response actions in MANET will isolates uncooperative nodes based on the node reputation factor derived from their behaviors. Such a simple and useful response against malicious nodes often neglects all the possible negative side effects involved with the response actions. In MANET scenario even improper countermeasures may cause the unexpected network partition, bringing the additional damages to the network infrastructure. To avoid the above mentioned critical issues, there should be more flexible and adaptive response decisions exist and investigated carefully.

The objective of this paper is to focus mainly on various routing protocols and risk mitigating techniques. The remainder of the paper is organized like this. Section II presents the key concepts of this paper. Section III presents existing risk mitigating techniques and section V concludes the paper with summary.

II. KEY CONCEPTS

The main concepts dealing in this paper are routing protocols, routing attacks and risk mitigating techniques.

A. Routing Protocol

The important task of the routing protocol is to discover the topology used to ensure that each node can acquire the recent map of the network to construct required routes to its destinations. Several efficient and effective routing protocols have been proposed for MANET. These protocols will generally fall into one of two vast categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols i.e) Ad hoc On Demand Distance Vector (AODV) protocol, nodes find the routes only when they must send data to the destination node whose route is unknown. In proactive routing protocols i.e) OLSR, nodes obtain the routes by periodic exchange of the topology information with other nodes and maintain all route information every time.

B. Routing Attacks

Based on the behavior of the attackers, attacks against the MANET can be classified into passive or active attacks. These attacks can be further categorized as either outsider or insider attacks. With respect to the target of the attacker node, attacks could be also divided into data packet or routing packet attacks. In the routing packet attacks, the attacker node could not only prevent existing paths from being used but also spoof the non existing paths to lure data packets to them. Several studies were carried out on modeling MANET routing attacks. Typical routing attacks include the black hole, fabrication, and modification of various fields in routing packets. All these above mentioned attacks could lead to serious network dysfunctions.

III. EXISTING RISK MITIGATING TECHNIQUES

The following risk mitigating techniques are currently available and used in the various Mobile Ad Hoc networks.

1. Packet leash is one of the mechanism for detecting and defending against routing attacks. A leash can be any information that is added to a packet and designed to restrict the packet's maximum allowed transmission distance. Leashes are of any of two types i.e.) Geographical leashes and Temporal leashes. The geographical leash ensures whether the recipient of the packet is within a certain distance from the sender. A temporal leash ensures whether the packet has an upper bound on its lifetime, hence it restricts the maximum travel distance because the packet can travel at most at the speed of light. Either the type of leash can prevent the routing attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows.

2. LAR is the reactive routing protocol like reactive routing protocol i.e) AODV and DSR. It helps to reduce the routing overheads that present in the traditional flooding algorithm by using location based information. This protocol hence assumes that each of the node knows its location through a Global Positioning System (GPS). Two different LAR schemes are available.

The first scheme will calculates a request zone which will define a boundary where the route request packets can travel to reach the required destination.

The second method will store the coordinates of the destination in the route request packets. These packets will travel only in the direction as the relative distance to the destination node becomes smaller as they travel from one hop to another.

Both schemes limit the control overhead transmitted through the network and hence it will conserve bandwidth. They also determine the shortest path to the destination node, since the route request packets travel away from the source node and toward the destination node. The worst disadvantage of this protocol is that each node is required to carry a GPS.

3. An intrusion detection system (IDS) or software application that monitors network and system activities for malicious activities and policy violations and based on that it will produce reports to a Management Station. Some systems may try to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Hence the Intrusion detection and prevention systems (IDPS) are always focused on identifying possible attack incidents, logging information about those incidents, and reporting attack attempts. All Intrusion Detection Systems use one of the two detection techniques: Statistical anomaly-based IDS and Signature-based IDS. A statistical anomaly-based IDS determines the normal network activity like what sort of bandwidth is generally has to be used, what protocols can be used, what ports and devices generally connect to each other- and alert the administrator or user when the traffic is detected which is not normal. Signature based IDS monitor's the packets in the Network and compares with pre-configured and pre-determined attack patterns that are known as signatures. There exist an issue that there will be lag between new threat discovered and the Signature being applied in IDS for detecting the threat.

4. Authenticated Routing for Ad hoc Network (ARAN) use the cryptographic certificates to offer routing security. At the beginning, it consists of a preliminary certification process and followed by a route instantiation process which guarantees end-to-end authentication. Ariadne can authenticate routing messages using any of three schemes: shared secrets that exist between each pair of nodes, shared secrets that exist between communicating nodes combined with broadcast authentication, or digital signatures. Using pair wise shared keys can avoid the need for synchronization, but it lead to the cost of higher key setup overhead; broadcast authentication such as TESLA will allow some additional protocol optimizations. Ariadne withstand node compromise and it relies only on highly efficient symmetric cryptography. Ariadne is hence more secure, more efficient, or more general (e.g., Ariadne does not require a trusted hardware and does not require powerful processors in any environment.

5. Anomaly detection scheme use dynamic training method in which the training data is updated at regular time intervals. In a blackhole attack, a malicious node might impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can hold the traffic from the source node. Hence it is necessary to prevent this kind of attack but it is very difficult to detect the abnormal behavior occurs during the attack. In conventional based schemes, anomaly detection can be achieved by defining the normal state from static training data. However, in mobile ad hoc networks since the network topology dynamically changes, such kind of static training method could not be used efficiently; hence dynamic training method is used.

METHOD USED	MERITS	DEMERITS
Packet leash method with TIK protocol	• Provides instant authentication of received packets. • TIK has computational and memory requirements that are easily satisfiable.	• Require broadcast authentication. • Precise time synchronization is not easily achievable.
Zone based Hierarchical model with AODV routing protocol	It allow only authenticate node to take part in route discovery	Restriction of collaborative attack is complex here.
Intrusion detection Method	Detect malicious node based on the	Risk of attack countermeasure is not

	behavior of node.	considered here.
Efficient symmetric cryptographic method with Ariadne which is a secure on demand routing protocol	No trusted environment needed	Routing protocol used here is less efficient than the optimized version of DSR
Dynamic learning method with AODV routing protocol	Training data can be updated according to the changing network environment	Updating training set is a tedious process.
Adaptive Probing technique with On demand secure Byzantine routing protocol.	Route discovery is Based on the aggregate signature.	Does not provide effective solution to the attacks other than the Byzantine attacks.
Dempster – Shafer Theory	Valuable tool for the evaluation of risk in engineering applications when it is not possible to obtain a precise measurement from experiments.	It does not support the non associative and weighted combination of rule which is required in most of the cases.

IV. CONCLUSION

Risk mitigating technique is one of the major issues in Mobile Ad Hoc environment. This paper surveyed the various existing Risk Mitigating techniques in MANET environment and compares their various parameters. Earlier Risk Mitigating technique does not consider the Risk because of countermeasure. Therefore there is a need to implement a new Risk Mitigating technique that can consider both the Risk because of attacks and Risk because of countermeasure in MANET environment.

REFERENCES

[1] Hu.Y, Perrig.A, and Johnson.D(2004), "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks*," Proc. IEEE INFOCOM, vol. 3, pp. 1976-1986.

[2] Radwan.A , Mahmoud.T , Houssein.E," Evaluation comparison of some ad hoc networks routing protocols".

[3] Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah," *A Survey on MANET Intrusion Detection*".

[4] Hu.Y, Perrig.A, and Johnson.D(2005), "*Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks*," Wireless Networks, vol. 11, no. 1, pp. 21-38.

[5] Kurosawa.S, Nakayama.H, Kato.N, and Jamalipour.A (2006), "*Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method*," Int'l J. Network Security, vol. 105, no. 627, pp. 65-68.

[6] Awerbuch.B, Curtmola.R, Holmer.D, C. Nita-Rotaru, and Rubens.H(2008), "*ODSBR An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks*," ACM Trans. Information and System Security, vol. 10, no. 4, pp. 1-35.

[7] Karlof.C and Wagner.D(2003), "*Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,*" Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315.

[8] Mohammed.N, Otrok.H, Wang.L, Debbabi.M, and Bhattacharya (2011, Jan./Feb), "*Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET*," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103.

[9] Marti.S, Giuli.T, Lai.K, and Baker.M (2000), "*Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*," Proc. ACM MobiCom, pp. 255-265.

[10] Praveen Joshi(2010)," Security issues in routing protocols in MANETs at network layer", WCIT.