A STUDY ON 'MOBILE AD-HOC NETWORKS'

KODALI VENKATESWARA RAO
Asst.Professor
Sri Sarathi Institute of Engineering and Technology
NUZVID
Krishna Dt. A.P

JALLURI GEETHA RENUKA
Asst.Professor
Sri Sarathi Institute of Engineering and Technology
NUZVID
Krishna Dt. A.P.

Abstract
Mobile ad-hoc network (MANET) has got tremendous success and attention due to its self- maintenance and self-configuration properties or behavior. Based on wired and wireless networks, the network topology of MANETs changes rapidly by means of routing attacks. Hence, providing security to this infrastructure-less network is a major issue. The routing protocols for ad-hoc networks cope well with the dynamically changing topology but are not designed to accommodate defense against malicious attacker. Malicious nodes have opportunities to modify or discard routing information or advertise fake routes to attract user data to go through themselves. In this article, we discuss a hybrid technique using anonymity, one-way trapdoor protocol, hash functions, and elliptic curve cryptographic to mitigate attacks in the MANET. The simulation is carried on NS-2 and the simulation results are dissected on different system execution measurements, for example, packet send and received, packet dropped, average network throughput, end-to-end delay, and packet delivery ratio.

Key Words: Asymmetric Authentication, Attacks, Key Exchange, Routing, Security, Wireless Network.

Introduction

Mobile unplanned networks (MANETs) square measure assortment of wireless mobile devices with restricted broadcast vary and resources. Communication is achieved by relaying knowledge on applicable routes that square measure dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes could be a major task, each from potency and security purpose of read. This paper presents a adept and secure routing, supported uneven authentication victimisation key exchange approach (KEA).

The proposed mechanism ensures secure routing and quality of service in MANETs and minimizes the network overhead. The KEA mechanism can be effectively used to develop a new routing protocol for Mobile Adhoc Networks which will provide maximum security against all kinds of attacks. In this paper, KEA is compared with other secure routing protocols like EEACK, AODV, and ARIADANE, to evaluate the efficiency of KEA in Ad Hoc Networks. The empirical results shows that there's a rise of 2 hundredth packet delivery quantitative relation and a discount of 100% routing overhead.

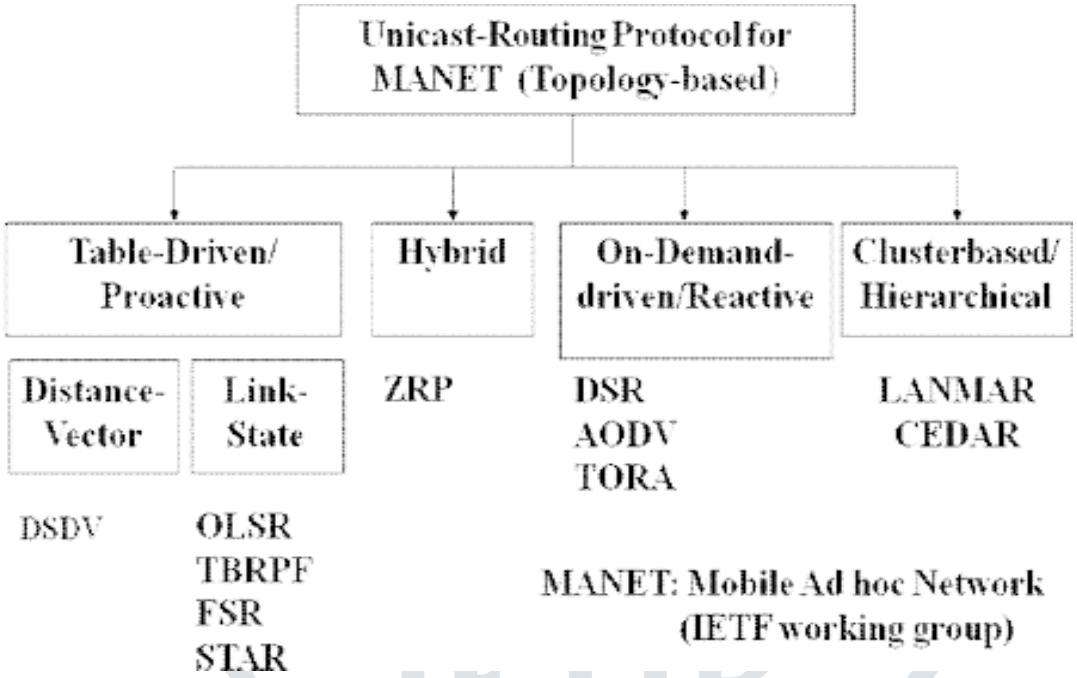
The network is localized, wherever all network activity, as well as discovering the topology and delivering messages should be dead by the nodes themselves. Hence routing practicality can got to be incorporated into the mobile nodes. Since the nodes communicate over wireless links, they need to deal with the consequences of radio communication, like noise, fading, and interference. In addition, the links usually have less information measure than a wired network.

The constellation is normally dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. An ad hoc wireless network ought to be able to handle the chance of getting mobile nodes, which will most likely increase the rate at which the network topology changes. Accordingly the network needs to be able to adapt quickly to changes within the constellation.

Routing protocols may generally be categorized as:

Table-driven OR Proactive routing protocols.
On-demand OR Reactive routing protocols.

Classification of Routing Protocols in MANETs



Network Security in Manets

Different variables have different impact on security issues and design. Especially environment, origin, range, quality of service and security criticality is variables that affect the security in the network. The ways to implement security vary if the range of the network varies. If the nodes are very far from each others, the risk of security attacks increases. On the other hand, if the nodes are so close to each others that they actually can have a physical contact, some secret information (e.g. secret keys) can be transmitted between the nodes without sending them on air. That would increase the level of security, because the physical communication lines are more secure than wireless communication lines. The last variable of Ad Hoc networks described with respect to security is security criticality. This means that before we think of the ways to implement security, we must consider carefully whether security is required at all or whether it matters or not if someone outside can see what packets are sent and what they contain. Is the network threatened if false packets are inserted and old packets are retransmitted? Security issues are not always critical, but it might cost a lot to ensure it. Sometimes there is trade-off between security and costs.

Problems with ad-hoc routing protocols

In ad-hoc routing protocols, nodes exchange information with each other about the network topology, because the nodes are also routers. This fact is also an important weakness because a compromised node could give bad information to redirect traffic or simply stop it. Moreover, we can say that routing protocols are very brittle in term of security. This part aims to provide a description of the causes of the problems with adhoc routing protocols. Infrastructure of ad-hoc networks

Ad-hoc networks have no predetermined fixed infrastructure, that‟s why the nodes themselves have to deal with the routing of packets. Each node relies on the other neighboring nodes to route packets for them.

Dynamic topology of ad-hoc networks

The organization of the nodes may change because of the mobility-aspect of ad-hoc networks: they contain nodes that may frequently change their locations. Because of this fact, we talk about the dynamic topology of these networks, which is a main characteristic that causes problems: when several adhoc networks mix together, there can be duplications of IP addresses, and resolving it is not so simple. Then, attacks can easily occur by using this duplication of IP address (cf. attacks using impersonation)

Problems associated with wireless communication

Wireless channels have a poor protection to noise and signal interferences, therefore routing related control messages can be tampered. A malicious intruder can just spy on the line, jam, interrupt or distort the information circulating within this network.

Implicit trust relationship between neighbors
Actual ad-hoc routing protocols suppose that all participants are honest. Then, this directly allows malicious nodes to operate and try to paralyze the whole network, just by providing wrong information.

Types of Attacks in MANET
Due to their particular architecture, ad-hoc networks are more easily attacked than wired network. We can distinguish two kinds of attack: the passive attacks and the active attacks. A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Instead, an active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The routing protocols in MANET are quite insecure because attackers can easily obtain information about network topology.

Attacks Using Modification
One of the simplest ways for a malicious node to disturb the good operation of an ad-hoc network is to announce better routes (to reach other nodes or just a specific one) than the other nodes. This kind of attack is based on the modification of the metric value for a route or by altering control message fields.

Attacks using impersonation
These attacks are called spoofing since the malicious node hides its real IP address or MAC addresses and uses another one. As current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take IP address of other node in the network and then use them to announce new route (with smallest metric) to the others nodes. By doing this, he can easily modify the network topology as he wants.

Security Threats in Network Layer
In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network.

Network Layer Attacks
A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow.

Attacks at different stages are as:

1. Attacks at the routing discovery phase
2. Attacks at the routing maintenance phase.
3. Attacks at data forwarding phase.
4. Attacks on particular routing protocols.

Attacks by Names are as:

1. Wormhole attack.
2. Black hole attack.
3. Byzantine attack.
4. Rushing attack.
5. Resource consumption attack.
6. Location disclosure attack.

Counter Measures
Security is a primary concern in MANET in order to provide protected communication between the communicating parties. It is essential for basic network functions like routing and packet forwarding. Network operation can easily be jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Hence, a variety of security mechanisms have been developed

to counter malicious attacks. There are two mechanisms which are widely used to protect the MANET from the attackers.

Security mechanisms

A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defense. As a second line of defense, intrusion detection systems and cooperation enforcement mechanisms implemented in MANET can also help to defend against attacks or enforce cooperation, reducing selfish node behavior.

Preventive mechanism

The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being hijacked. The protection of the sensitive data on a physical device can be enforced by some security modules, such as tokens or a smart card that is accessible through PIN, pass phrases, or biometrics. Although all of these cryptographic primitives combined can prevent most attacks in theory,in reality, due to the design, implementation, or selection of protocols and physical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms.

Reactive mechanism

An intrusion detection system is a second line of defense. There are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behavior based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behavior statistically. It collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. In practice, both approaches can be combined to be more effective against attacks. Some intrusion detection systems for MANET have been proposed in recent research papers.

Countermeasures on Network Layer Attacks

Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. Use of secure routing protocols provides the first line of defense. The active attack like modification of routing messages can be prevented through source authentication and message integrity mechanism. For example, digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain is used for this purpose. By an unalterable and independent physical metric such as time delay or geographical location can be used to detect wormhole attack. For example, packet leashes are used to combat this attack. IPSec is most commonly used on the network layer in internet that could be used in MANET to provide certain level of confidentiality. The secure routing protocol named ARAN protects from various attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source rout etc.

The passive attack on routing information can be countered with the same methods that protect data traffic. Someactive attacks, such as illegal modification of routing messages, can be prevented by mechanisms source authentication and message integrity. DoS attacks on a routing protocol could take many forms. DoS attacks can be limited by preventing the attacker from inserting routing loops, enforcing the maximum route length that a packet should travel, or using some other active approaches. The wormhole attack can be detected by an unalterable and independent physical metric, such as time delay or geographical location. For example, packet leashes are used to combat wormhole attacks.

In general, some kind of authentication and integrity mechanism, either the hop-by- hop or the end-to- end approach, is used to ensure the correctness of routing information. For instance, digital signature, one-way hash function, hash chain, message authentication code (MAC), and hashed message authentication code (HMAC) are widely used for this purpose. IPsec and ESP are standards of security protocols on the network layer used in the Internet that could also be used in MANET, in certain circumstances, to provide network layer data packet authentication, and a certain level of confidentiality; in addition, some protocols are designed to defend against

selfish nodes, which intend to save resources and avoid network cooperation. Some secure routing protocols have been proposed in MANET in recent papers. We outline those defense techniques at below sections.

Countermeasures for wormhole attacks

A packet leash protocol is designed as a countermeasure to the wormhole attack. The SECTOR mechanism is proposed to detect wormholes without the need of clock synchronization. Directional antennas are also proposed to prevent wormhole attacks. In the wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. To defend against wormhole attacks, some efforts have been put into hardware design and signal processing techniques. If data bits are transferred in some special modulating method known only to the neighbor nodes, they are resistant to closed wormholes. Another potential solution is to integrate the prevention methods into intrusion detection systems. However, it is difficult to isolate the attacker with a software-only assumptions on Security can be made.

References

1. Amit Kumar "A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization" International Journal of Computer Science and Mobile Computing, 2015. Pp 80-85.
2. JuhiViswas, Ajay Gupta, Dayashankar Singh" WADP: A Wormhole Attack Detection Andprevention Technique in MANET using Modified AODV routing protocol" IEEE, 2013. Pp 376-381.
3. Issa Khalil, SaurabhBagchi, Ness B. Shroff "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks" Elsevier ltd. 2007, Pp 344-362.
4. BadranAwad, TawfiqBarhoom "BT-WAP: Wormhole Attack Prevention Modelin MANET Based on Hop-Count" IJARCCE, 2015. Pp 600-606.
5. Rakhil R, Rani Koshy "An Efficient Algorithm for Neighbor Discovery and Wormhole Attack Detection in WANET"2015 International Conference on Control, Communication & Computing India (ICCC) 19-21 november 2015.
6. Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" IEEE, 2008. Pp 343-348.
7. AnjuJ,Sminesh C N,"An Improved Clustering-based Approach for Wormhole Attack Detection in MANET" 3rd International Conference on Eco-friendly Computing and Communication Systems 2014.
8. S. Choi, D. Kim, J. Jung. "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks". In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2008.
9. J. Eriksson, S. V. Krishnamurthy, M Faloutsos "Truelink: A practical countermeasure to the wormhole attack in wireless networks" 2006, Pp 75–84.
10. W. Wang, B. Bhargava, Y. Lu, X. Wu "Defending against wormhole attacks in mobile ad hoc networks: Research articles" Wireless. Commun.Mob.Comput. 2006, Pp 483–503.
11. Kamanshis Biswas, Md. Liakat Ali. "Security Threats in Mobile Ad Hoc Network". Paper submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology, 2007.
12. Y.-C. Hu, D.B. Johnson. "Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks", Wireless Networks, 11(1-2), 2005.
13. Bounpadith Kannhavong, Hidehisa Nakayama, Abbas Jamalipour. "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communication, 2007.
14. R. Graaf, I. Hegazy, J. Horton. "Detection of wormhole attacks in wireless sensor networks," Springer book chapter Ad Hoc Networks, 2010.