Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July, 2021:1340 – 1349

A survey on Security Challenges in Mobile Ad hoc Networks

C. Edwin Singh[a], Dr. J. Amar Pratap Singh [b]

[a] Research Scholar,[b] Professor,
Computer Science & EngineeringComputer Science & Engineering, NICHE, Nagercoil.NICHE, Nagercoil

Abstract

MANETs (Mobile Ad hoc Networks) is an infrastructure-less network in which mobile acts as a node, which is deployed for Mobile to Mobile communication and with Base Station (BS) to exchange information. MANETs helps in various activities such as military camps, disaster situations and in emergency situation etc. Due to the lack of infrastructure networks in MANETs, there is a high probability of security issues such as collision attack, man in the middle attack, authentication issues, establishing a reliable end-to-end communication path, and secure data transfer, etc. In this survey, we have discussed the security challenges to be faced while the deployment MANETs. Also, we discussed the four main aspects to be concentrated on to provide secure communication. The four main aspects are Routing – a selection of routes which provide reliability and unlink ability, Key Sharing – the most important aspect to provide a secure and attack free network, Authentication – Authentication of nodes in a network, Security – Data transfer. In this survey, we have concentrated on all four aspects of the network and analyzed to provide a secure and attack-free network

Keywords: MANET, IDS, Authentication, Routing, Attacks.

1. Introduction

Mobile ad-hoc networks [1] (MANETs) technology is an emerging technology for the last few years. MANET is originally to reflect the ad hoc nature of the highly dynamic nature of networks. MANETs are dynamic nature of network which is created for establishing a network for a specific need or situation. Nowadays MANETs are established as reliable networks to communicate between Mobiles on highways or urban environments in specific or needy situations. MANETs are no infrastructure in nature that needs to connect with other Mobiles and pass information in emergency situations. Lack of infrastructure loads an additional burden for MANETs. In MANETs, every Mobile acts as a node in a network and manages and controls the communication in a network. MANETs are mostly used for Mobile to Mobile communication (M2M) and a Mobile to Base Station (BS) or as also called Mobile to Infrastructure (V2I) based on local wireless networking technology. This main contribution of this paper is to discuss a detailed survey about the challenges in MANET regarding communication and the threats and attacks on MANETs and remedies taken in previously addressed works. Here we also address the security and privacy issues in MANETs because these are critical to system dependability and customer acceptance. Finally, this paper summarizes the state-of-art of MANETs and discusses the open issues of MANETs.

MANET [2] contains nodes that communicate with each other without infrastructures i.e., without a central network, and nodes are equipped with network capabilities. MANET on the other side has emerged as a challenging and more liable class or variation of MANET. MANET provides inter Mobile communication to pass and receive information so that it helps in military camps for passing secured information, detect student presence in school/college, detect emergency situations, and overall to provide a better solution.

2. Architecture

MANET [2] aims to provide communication between different neighboring Mobiles. The MANET can be divided into three domains.

1)Mobile domain: Mobile domain consists of two parts. The first part is all the moving Mobiles. The second part is the mobile device which contains handy devices like PDAs, GPS, smart phones, etc.

2)Infrastructure domain: The infrastructure domain also consists of two parts. The first part is Base Station and the second part is the central infrastructure which includes the central managing center such as the Mobile management center.

3)Generic domain: The generic domain consists of Internet infrastructure and Private infrastructure. The different nodes and servers and the other computing devices work directly or indirectly for a MANET.

From the above three types of domains, the information is shared between the mobile domain to the infrastructure domain and in the next step the infrastructure domain shares the information to a generic domain such as the information and messages are shared between them. The flows of data among the fixed and mobile resources result in better efficient and effective utilization by road users to increase road traffic efficiency.

Another form of MANET architecture [2] is communication architecture where communication types are characterized into 4 sections. They are

1) In Mobile communication: It is an inner system data communication that helps to maintain the performance of the Mobile like informing the critical situations and emergency needs.

2) Mobile to Mobile communication (M2M): This communication takes place between two Mobiles which assists the users to share secret information and critical situations. M2M does not rely on fixed infrastructure. Form a network at the time of need.

3) Mobile-to- infrastructure (M2I) communication: The data exchange between the Mobile and the Base Station (BS). This communication is useful to request secure keys and authentication.

4) Mobile-to-broadband cloud (M2B) communication: This communication is between Mobile and the internet 3G/4G. This is mostly used to track the Mobile.

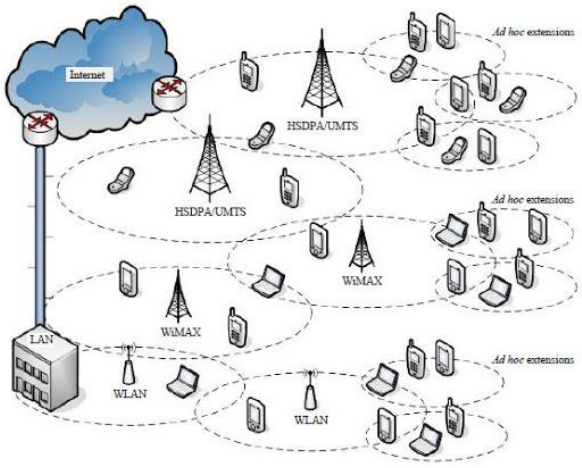

Figure 2.1 MANET Architecture

2.1 Applications of MANET

MANET [2] is deployed in the real world for numerous advantageous applications. So of the applications are listed below

a) Military Sector: To maintain the network information between the soldiers, vehicles, and military information headquarters.

b) Commercial Sector: MANETS are mainly used in disaster relief such as floods, fire, and earthquakes.

c) Low Level: Used to communicate with the home networks where devices communicate to exchange their data.

d) Data Networks: MANETS in commercial applications needs high-level computing of data, this allowing computers to compute and forward data to others.

e) Sensor Networks: These types are used in detection mostly. Examples include temperature, pressure, toxins, rainfall, pollutions, etc.

2.2 Characteristics of MANET

MANET[2][3] has its own distinct characteristics which are listed as follows.

a) High Mobility: The movement of nodes in MANETS is very high, which makes it harder to predict the position of each node and provide security to each node's privacy.

b) Unpredictable Network topology: MANETs are infrastructure-less with high mobility, the position of the nodes frequently changes, which results that network topology frequently changes.

c) Unbounded network size: The MANETs are geographically unbounded, which are implemented in several cities and connecting countries.

d) Adequate information sharing: There is a need to share information from RSU to Mobiles and Mobile to Mobiles which results in excessive amounts sharing between nodes is frequent.

e) Wireless Communication: MANETs are designed for wireless environments. MANETs are interconnected and exchange their information via wireless.

f) Time Critical: There is a very short time limit for sharing information between nodes to be delivered.

g) Sufficient Energy: Normally Mobiles and RSU units are equipped with sufficient energy with built-in battery resources. This helps to use demanding techniques RSA, ECDSA, etc.

h) Physical Protection: MANETs are high protected than MANETs in nature, MANETs nodes are more difficult to compromise.

Before deployment of MANET [3], we should consider some of the security requirements to perform for a secured and attack free environment for sharing. Here some of the security requirements are listed which are common and some or specific to MANET. They are

a) Authentication: Main requirement of MANET. This ensures that the message or request user is a legitimate user. Failure of this requirement leads to heavy attacks. Three types of attributes are used for authentication of nodes on participation in a network or while communicating. They are ID authentication, Property Authentication, Location Authentication.

b) Integrity: This is also a major requirement of MANET. This ensures that the message is received by that authenticated user and ensures that the message is not tampered or not altered or unauthorized creation of data.

c) Confidentiality: On communication between nodes or BS the message should be secured, such that the outsiders in a network or other than the sender and receiver should not able to understand the confidential information.

d) Availability: The network and application should remain in the presence of critical situations like attacks or faults. The network should be fault-tolerant.

e) Access control: Determining the roles and privileges for the messages and nodes such as the sensitive communication by military and military head office services should not be heard by the other nodes in a network.

f) Unlinkability: This is also one of the major characteristics while communicating from one node to another node, In MANET a route is formed, in route number of nodes occurs between the source and destination. This characteristic ensures that the participated nodes in a network should identify that this source and destination are communicating.

2.3 Attackers On Mobile Network

To secure a network we should have strong knowledge about the attackers and the type of attackers that collapses the network and which ways they attacks. In MANET [3][5] the attackers are classified into three categories.

a)Insider and Outsider: Insider attackers are who the ones are authenticated and participate in the network. Outsider attackers are the intruders.

b)Malicious and Rational: Malicious attackers are doing not gain to attack, they just harm the functionality of the network, whereas rational attacks gains on the attack, and they are unpredictable. The rational attackers are who steal data, tampers, or replaces the data while communicating.

c)Active and Passive: Active attackers generate signals and packets and participate in the network while the

passive attackers just only sense the work.

2.4 Attacks In The Manet

To form an attacker free network and secure communication [3][5] we should have knowledge about the various types of attack by the network and when it occurs and by the type of attackers.

a)Impersonate: In impersonate, attack attacker assumes the identity and privileges of an authorized node.

b)Session hijacking: Most authentication process is done at the start of the session. In this attack, attackers take control of the session between nodes

c)Identity revealing: Generally a driver is itself owner of the Mobiles hence getting the owner's identity can put the privacy at risk

d)Repudiation: The main threat in repudiation is denial or attempt to denial by a node involved in communication.

e)Eavesdropping: It is the most common attack on confidentiality. The main goal of this attack is to get access to confidential data

f)Denial of Service: In this attack, the attacker prevents the legitimate user to use the service from the victim node

2.5 Solutions of Security And Privacy For MANETS

On considering the above-listed attacks we have to deploy secured and authenticated MANETs. But concentrating on all the aspects of attacks it is a tedious process to develop such an environment.

3. Routing

Routing [6][7] is the heart of the MANETs. To form a network in such an environment (infrastructure less) routing is more essential. Selecting a secured and authenticated routing is a tedious process. Here Routing plays an important role. Since via routing only the sharing of keys and the message communication is done. If forming a route with legitimate nodes helps to form a secured and authenticated network and secured key sharing and communication. Also selecting of routing protocol for MANETs not only a security concern we should look into some of the features like routing supporting environment, Forwarding strategy, Predictive, Buffering, Overlay, and non-overlay and positioning system. To form such routes number of proposals were called, which are listed below this section.

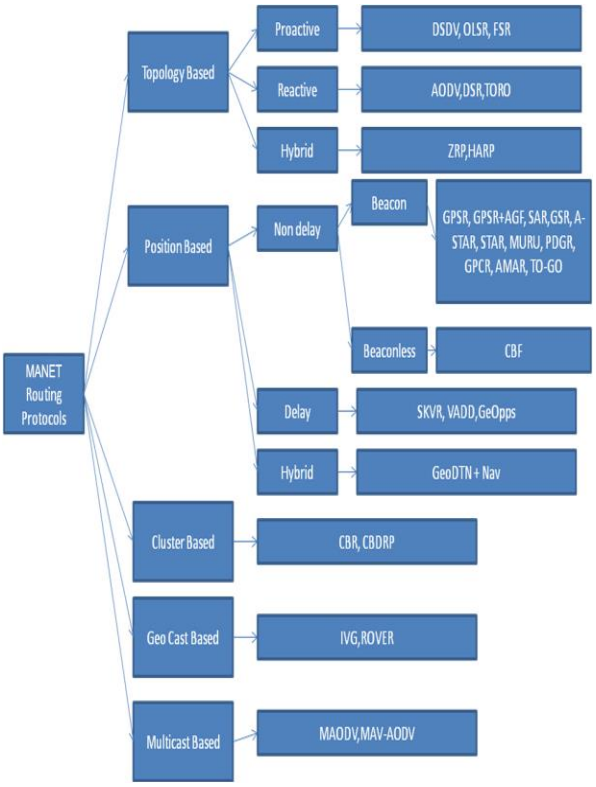

Figure 3.1 Routing Protocols

3.1 Overview of Key Sharing in MANETS

Key sharing [8],[9] an important aspect of MANETs to develop a secured and authenticated MANETS. Previous studies stated the key sharing in MANETs is a tedious task which is elaborated on how the key is shared between the nodes or between the sender and receiver. The key is the main part for authentication of nodes and securing the messages between them. Various constrain like the mobility of MANETs, computational complexity, dynamic movement of MANETs, low capacity makes the environment more risk to security attacks. Considering the above constrain of MANETs the key should be generated and shared between the nodes.

The keys are broadly classified as follows

Symmetric Schemes

Symmetric key [8] uses a private key infrastructure concept which has a common key between the nodes. The symmetric key is also known as private key cryptography uses the same key for encryption and decryption. In MANETs, most of the existing schemes use symmetric key sets that are drawn from the key pool and shared by the members from the key pool. However, the symmetric schemes have the main drawback which does not ensure non-repudiation

b) Asymmetric Schemes

Asymmetric key uses public key infrastructure which holds a pair of keys i.e., public and the private key used to encrypt and decrypt messages to ensure data security. Here in the asymmetric scheme, the public key is used to encrypt the message or which is used to verify the signature whereas the private key is used to decrypt the message and used to create a digital signature. Both the public key and private keys are mathematically linked. Most of the MANETs schemes use ID-based schemes that use identity such as name, email address, etc., for public-key verifications. Most Identity-Based Schemes are based on bilinear pairing or discrete logarithmic problem for pairing in groups. In the deep study, most of the researchers use an ID-based scheme for encryption and authentication. This scheme efficiently improves computation and communication. RSA, ECC, and Elliptic curve digital signature algorithm (ECDSA) are the three frequently and mostly used asymmetric algorithms. On comparing with the symmetric algorithm asymmetric cryptography algorithm is slower in the computational process due to the nature of the complexity of the algorithm.

c) Hybrid Schemes

Since due to the lack of non-repudiation in symmetric schemes, if a key is discovered or intercepted by the attackers, which leads to a chance of stealing the data. Also in Asymmetric algorithm is slower due to the complexity of the algorithm. Regarding the above issues stated in symmetric and asymmetric algorithms some of the researches use a combination of symmetric and Asymmetric key management which uses according to the different phases of the scheme. In the hybrid scheme, the asymmetric scheme is used to ensure the privacy of the messages and authenticate it, whereas the symmetric scheme is used in periodical messages send between RSU and nodes.

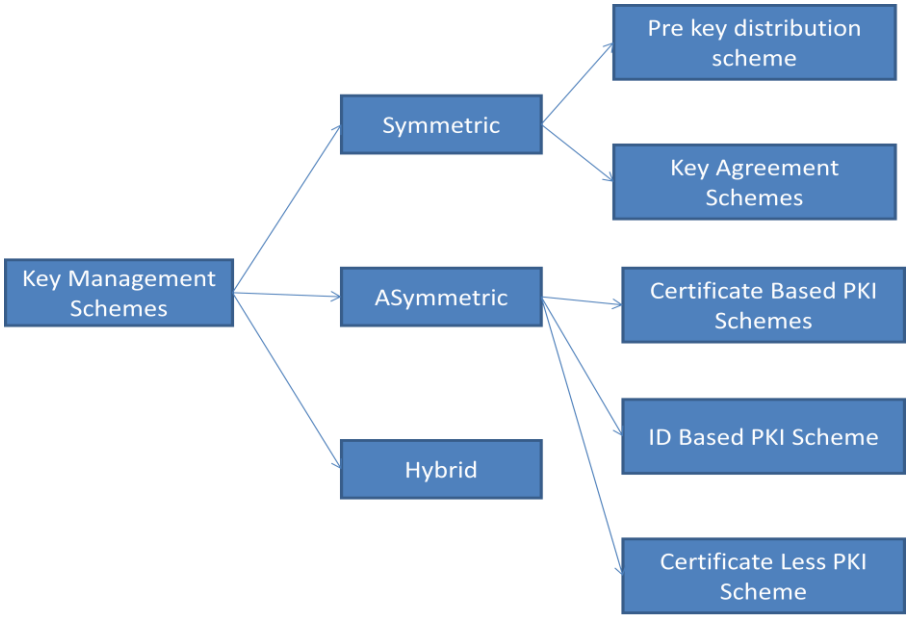

Figure 3.2 Key Management Schemes

From the above key management tree each key type having different schemes used for key sharing. In MANETs the key sharing plays a vital role. But previous studies and existing works mostly use both Symmetric and Asymmetric but the main factor is how keys are shared securely to the source and destination for authentication and key sharing. If the keys are shared using a Pre-shared scheme which leads to vulnerable attacks such as (Brute force Attack, Replay Attack, etc). Also, we need to take into account when the keys to be shared and renewal new keys once the communication ends which helps keep the VANATs to avoid vulnerable attacks and maintain security.

3.2 Overview of Authentication in MANETS

Authentication [7][8][9] is an important feature for MANET which is used to verify the authenticity of a user and the data transmission to avoid unauthorized access and the attackers. In MANETs, while designing the authentication scheme six main requirements should be taken into the account. First, all the authentication should be done in real-time which incurs more time delay, In MANETs to ensure the time delay which is a tedious process and should take into account. Secondly, Anonymity used to ensure privacy and the authentication scheme should be designed such as anonymity is maintained. Thirdly, non-repudiation must be considered while designing the authentication scheme. Fourth, the nature of the network in MANETs the nodes are not static which is highly movable, and infrastructure-less, so mobility should be considered. Fifth, the storage of security credentials in Mobiles may subject to tampered and finally the accuracy of data.

3.3 Goals of Authentication

In addition to the message authentication in MANETs, there are certain goals to be considered in-depth which are not reviewed by several authentication schemes.

a)Privacy (integrity): Each and every node (Mobile) in a network should be protected against unauthorized and identifying observations.

b)Real-time constraints: Due to the infrastructure less and high mobility nature of MANETs, timely communications should be considered and should be strictly taken into the account.

c)Non-repudiation: In critical situations or when needed, the scheme should be designed such that or allowed to check the identity of the Mobile by their sending messages to the destination Mobile without denying.

d)Infrastructure independency: In the unavailability of RSUs in some situations, the scheme should avoid frequent access to a network to perform authentication.

3.4 Authentication Schemes

Mostly the recent authentication schemes mainly focus on the following objectives, to reduce communication overhead, anonymity, to isolate misbehaving nodes, and non-repudiation services. Most of the works concentrate on these things commonly and lack of main perspectives and these may be appropriate

objectives to their scheme.

The existing authentication schemes are classified into three main types

a) Asymmetric Key Authentication Scheme

b) Symmetric Key Authentication Scheme

c) Infrastructure requirement

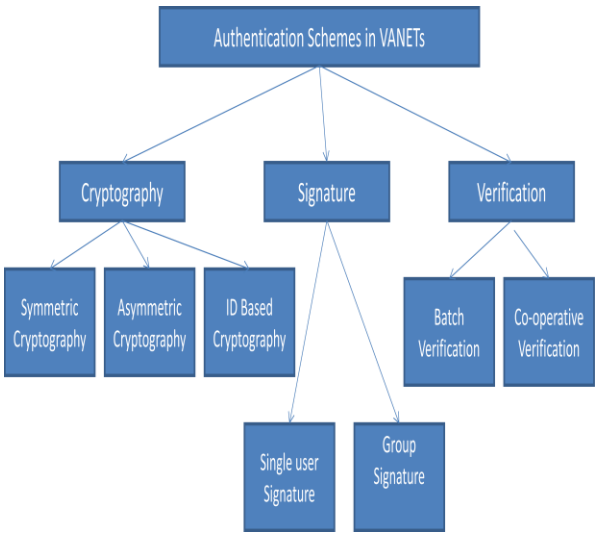

Figure 3.3 Authentication Schemes

a) Asymmetric Key Authentication Scheme

This is a traditional and well-known scheme mostly used scheme for authentication. This uses key pairs (public/private keys) and digital signatures for authentication of nodes. This is categorized into two sub categories.

i) Group based Schemes

A group is formed between the members and a group manager holds the group of public-key which maps to multiple private keys is distributed to each member in a group for authentication. The group manager decides to determine which private keys sign a message. Below this list of group-based schemes are illustrated.

1) PPAA

The peer-to-peer anonymous authentication scheme proposed by Tsang and Smith forms a P2P system between MANETs. PPAA is a credential-based system that balances privacy and accountability. But the main lack is no two instances of registration can be run concurrently.

2) Efficient and Robust pseudonymous authentication

It is a hybrid scheme of MANETs to provide high security and authentication. To provide high-end secured authentication to deploy safety applications of MANET pseudonymous and group signatures are combined. The main objective of this approach is to provide message authentication between nodes, integrity, non-repudiation service, anonymity, and avoids linking of multiple messages to a single node. Here the pseudonyms are used to verify the messages. But however, this scheme is lack in robustness. To reduce overhead and increase robustness using the same approach three optimizations were done. These three optimization works conversely decrease robustness but still, the system relays on revocation lists which causes an increase of overhead between nodes.

3) GSIS

The scheme is proposed to address the security assurance and privacy preservation in MANETs for this it employs a novel scheme a combination of Group signature and Identity-based Signatures (GSIS). The GSIS scheme provides data origin authentication, integrity, the anonymity of user authentication and ID, prevents replication, and avoids Mobile traceability. GSIS is relatively efficient comparing other schemes. But the main

drawback of GSIS is on simulation loss of message increases the number of Mobiles within the communication range also increases.

4) TACK

Temporary anonymous certified keys(TACK) are developed to provide privacy, short-term linkability, traceability and revocation, and efficiency. Comparatively no other schemes provide all these features at the same time. TACK is based on standard asymmetric techniques and group signature schemes but mainly depends on the infrastructure as it divides the roadways into geographic regions. Since this scheme mostly relies on infrastructure for providing security which is not suitable for several concepts and assumptions. On the other hand, the TACK does not limit the communication overhead.

5) Probabilistic adaptive anonymous

The group-based anonymous authentication addresses the higher need for anonymity and provides a typical authentication scheme. Here in the scheme, RSUs are appointed to perform authentication tasks, use public-key cryptography. This scheme prevents central authentication overheads. The primary advantage of this scheme is adjustable levels of privacy. The major drawback is again a heavy dependency on infrastructure.

ii) Non-Group based Schemes.

Each node is equipped with separate public and private key(key pair) for authenticating/verifying the digital signatures.

1) SRAAC

Secure Revocable anonymous authenticated inter-Mobile communication scheme is designed is to improve the following security issues such as to protect message unlinkability, to rely on single CA for all authentication certificates, OBU memory, and bandwidth usage. Using this scheme unlinkability and anonymity are achieved along the scheme reduces memory and bandwidth consumption. The major drawback is when a malicious node is identified which is not quickly isolated or removed from the network.

2) An Identity based secured framework

The identity based secured framework is proposed to heavy the reliance on public-key cryptography and pseudonym assignments. Also, the delay between two nodes also considered in this scheme. Unfortunately, most of the computations and storage are done in the Base station; it is responsible for revocations and revocation checking. This is the major drawback of identity based secured framework.

b) Symmetric Key Authentication Scheme

This authentication scheme is also one of the traditional which is commonly used. This scheme uses a shared key between the authenticator and verifier. This scheme is also categorized into two subcategories.

i) Group based Schemes

A shared key is used among a group for authentication and group communication.

1) PPGCV

Privacy preserving group communication scheme for MANETs (PPGCV) is one of the few works for group communications in MANETs. PPGCV is proposed to satisfy the following requirements in MANETs such as forward and backward secrecy, authentication, protection against collision, and privacy. This approach minimally relies on network infrastructure. The major drawback of the PPGCV scheme is each node and server needs high storage requirements in order to store the keys for the rekeying phase. Lack of speed and efficiency.

2) TARI

TARI is a group based symmetric key authentication scheme which is proposed based on TACK(Asymmetric scheme). Same security goals are proposed as of TACK the difference is TACK uses Asymmetric keys and TARI uses symmetric keys. The same drawback of TACK is also occurred in TARI. Delay overhead is very high.

ii) Non-Group based Schemes

Each node is equipped with a separate shared key for authenticating/verifying the communication messages.

1) VAST

VAST utilizes ECC(Elliptic Curve cryptography) with Tesla++ which is a modified version of Tesla. VAST is also minimal infrastructure support. Since it's minimal infrastructure support it is supported to deploy in any areas. However, the main drawback of delay to authenticate the messages and nodes.

2) An efficient message authentication scheme for MANETs

It is a new message authentication scheme proposed to secure the following conditions. They are message integrity and source authentication, low communication overhead and fast verification, privacy preservation, Prevention of internal attacks. The proposed scheme is delivered with a combination of two schemes namely COMET and RAISE. The main drawback of the scheme is which does not provide any mechanism to revoke the keys.

c) Infrastructure requirement

This authentication is done based on infrastructure a node is authenticated while joining the network and also verified whenever the node in need of resources related to infrastructure such as keys, revoking of keys, certificates, and new key generation, etc,.

3.5 Comparison and Issues Related To Secure Authentication Protocol For MANETS

During our survey, we have seen the three main concepts of MANETS to provide a secure and authenticated and collision-free environment, The three main concepts took is secured and authenticated routing, Key sharing, and the authentication protocols. Upon choosing the three concepts we have to take a look at the different attributes to provide an efficient and secured authentication protocol, they are Security, Integrity, Non-repudiation, forward and backward secrecy, unlinkability, anonymity, collusion-free, and moreover energy efficient and uses less storage. Upon considering all the attributes to develop a secure and authentication scheme for MANETs is a tedious process. Since if we concentrate on security and authentication there will be a lack of energy and storage and collusion. If we concentrate on collusion it will incurs high energy and lack of anonymity and incurs high storage and uses high network and depends on infrastructure. From our survey choosing each protocol and combining is tedious work, In the routing part, overall AODV is a comparatively secure way of routing and lacks security and authentication which can improve by using key sharing technologies and should provide anonymity and unlinkability. Secondly upon choosing key sharing concepts a combination of asymmetric and the symmetric key is the best way and also we need to choose an encryption/decryption algorithm which should not take much time to encrypt/decrypt. Thirdly authentication is the main part of MANET which avoids unauthorized and malicious nodes in the network and while key sharing and checking the integrity of nodes. Also, we have to take the time factor into the account while authenticating each and every node and the messages it should not incur more time and storage if so it will lead to high traffic in a network. Also, an elegant method of authentication should be chosen which highly depends upon the key sharing method.

4. Conclusion

Communication between Mobiles has become more critical for car designers and manufacturers in the future. The Mobile ad hoc technology offers communication services for Mobiles but still need improvement and enhancement. Also to avoid a collision-free network an authenticated routing and efficient key sharing network is to be chosen. In this survey, we have discussed the factors of authentication, routing, and key sharing techniques of MANETs to develop an authenticated and efficient routing that avoids collision attacks and isolates malicious nodes. But considering the above survey if some routing protocols achieve security and authentication which lacks resources and storage and efficiency. So no other protocols are designed to achieve both security and efficiency in all aspects.

References

[1] Marcelo G. Rubinstein (2006), "A Survey on Wireless Ad Hoc Networks" Mobile and Wireless Communication Networks pp 1-33, 2006

[2] Jeroen Hoebeke (2004) "An overview of mobile ad hoc networks: Applications and challenges " Journal of communication networks July 2004

[3] D Djenouri, L Khelladi (2005), "A survey of security issues in mobile ad hoc and sensor networks" IEEE Communications Surveys and Tutorials 2005

[4] Ali Dorri, Seyed Reza Kamel, Esmaeil Kheirkhah (2015), "Security challenges in mobile ad hoc networks:a survey" Networking and Internet Architecture 2015.

[5] Felipe (2014), "Data communication in MANETS: A survey, Challenges and Applications", March 2014

[6] Sunil Taneja and Ashwani Kush (2010), "A Survey of Routing Protocols in Mobile Ad Hoc Networks" International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010

[7] H Füßler (2002), "A comparison of routing strategies for vehicular ad hoc networks", 004 Computer science, internet 2002

[8] Vu Khanh Quy (2019), "Survey of Recent Routing Metrics and Protocols for Mobile Ad-Hoc Networks" Journal of Communications Vol. 14, No. 2, February 2019.

[9] Al-Sakib Khan Pathan (2010), "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET",ACM Transactions may 2010.