A Frame Work to Estimate the Performance of Authentication Schemes in Mobile Ad Hoc Networks

Deepak Kumar
Research Scholar
Department of Computer Science
Faculty of Technology
Gurukul Kangri
Vishwavidyalaya, Haridwar
Uttarakhand, India

Vinod Kumar, PhD
Professor
Department of Computer Science
Faculty of Technology
Gurukul Kangri
Vishwavidyalaya,Haridwar,
Uttarakhand, India

ABSTRACT
An increasing growth has been witnessed in the last few year with respect to development of wireless and mobile communication networks. In MANETs, nodes are able to communicate through the use of wireless mediums, constituting dynamic topologies. The certificate-based authentication has a positive edge in wired networks. It's a significantly arduous task to adapt a certificate based authentication protocols for mobile ad hoc networks due to absence of fixed infrastructure or centralized management. A traditional certificate-based authentication system depends on a fixed trusted Certificate Authority (CA). In this case Certificate Authority (CA) takes the responsibility for the establishment, distribution, renewing, and revocation of certificates. The consideration of the fixed centralized network is not practically possible in MANETs, because of issues such as regular link breakdown, node mobility, and inadequate wireless medium. The numbers of approaches have been introduced, which focus on the challenges to adapt certificate-based authentication in a distributed way in mobile ad hoc networks. In this paper, some issues related to performance analysis of exiting authentication schemes have been discussed.

So, there is a need to construct a common frame work to evaluate the performance of certificate based authentication protocols for MANETs. This framework is based on two pillars. One is to survey some of the existing authentication mechanisms for MANETs and identify the needs of a secure authentication mechanism for MANETs in the context of distributed authentication. Second is the derivation of metrics to evaluate the performance of certificate based authentication schemes is done.

Keywords
Authentication schemes, ad-hoc and sensor networks, mobility model, metrics evaluation.

1. INTRODUCTION
The several challenging issues are present in the deployment of security mechanism for MANETs, due to the arbitrary topology, the dynamic nature of the nodes, the transmission errors and limited wireless range of nodes. Since all the nodes collaboratively work to forward the data in the network, the wireless channel is prone to passive and active attacks by malicious nodes, namely, eavesdropping, spoofing, Denial of Service (DoS), etc. Implementing security is therefore a most prominent task in MANETs.

The components of a security mechanism are integrity, confidentiality, availability, authenticity and non-reputability. The authenticity is the most important issue of concern since violation of authenticity directs to a system-wide compromise. The widely used authentication mechanisms in traditional wired networks are the public key management system using certificates. The certificate-based schemes have emphasized on the protected distribution of the public keys. The PKI defines method to deal with public key management using X.509 certificate [1]. In wired network the centralized certificate server handles different phases of certificate like construction, revocation and renewal of certificates. This is not duly considered in ad hoc networks due to the nonexistence of a fixed infrastructure and centralized management. The existence of dynamic topology may reflect the frequent link failures resulting in issues such as timely communication with the certificate server and re-authentication.

Several existing public key management mechanisms cope up with these limitations and reap full advantage of the certificate-based authentication mechanism [2-7]. In this paper, some of the certificate based authentication schemes have been discussed with their merits and demerits.

The remaining paper is organized as follows. In Section 2, security and key management issues are discussed. Section 3 comprises the needs of certificate based authentication schemes with brief description of the applied mechanisms. In section 4, a comparison matrix has also been made with respect to the requirements of applied authentication mechanism. Section 5 provides metrics for evaluation of certificate based mechanisms. In section 6, performance analysis of secure AODV routing protocol in battlefield scenario is discussed.

2. OVERVIEW OF KEY MANAGEMENT SCHEMES
Unlike wired network, the dynamic nature of ad hoc networks leaves them vulnerable to security attacks. Every node act both as a router and communication end point. This makes the network layer more prone to security attacks. A main challenge is to verify the authenticity of routing message. The general assumption is that node possession of valid secret key can be trusted. Consequently, a proper key management service is required. The key management service required for application layer security as well as for protection of network layer. Anne Marie [19] proposed taxonomy of key management schemes that can be achieved in several ways. Here, two main categories, namely contributory and distributive are proposed. In distributive category each key originates from a single node. The nodes may nicely cooperate during key distribution. Distributive schemes may be distributed or centralized. In the distributed schemes, every node generates a key and attempts to distribute it to others while in contributory schemes the key is the outcome of a mutual effort of more nodes. Some of the contributory schemes depend on a centralized entity, others do not. The

categories "contributory" and "distributive" are reflected in some of the authentication schemes for Ad hoc networks. The classification of key management is illustrated in Fgure 1. The distributive key scheme is further classified into public key and symmetric key schemes. The public key schemes include traditional certificate-based and identity-based schemes while the symmetric schemes may consider to perform authentication in MANET or wireless sensor networks (WSN). WSNs describe a new class of ad hoc networks with better self controlled nodes than traditional MANETs. Contributory schemes are characterized by the absence of a trusted third party accountable for distribution and generation of the cryptographic keys.

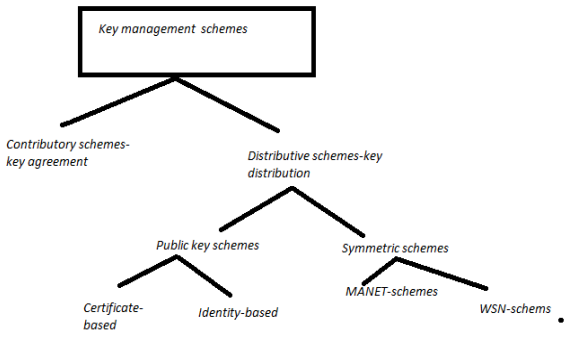


Figure-1 Key management schemes

Rather than, all communicating entities participate to establish (i.e., "Agree" upon) a secret symmetric key. The number of participants ranges from two parties (establishing a pair wise key) to many parties (establishing a group key). The contributory approach may be adopted for ad hoc network. Truly ad hoc networks require the trusted entity to be established spontaneously during network initialization. The public key distribution in certificate based authentication schemes is to be accomplished in such a way that it allows the receiving nodes to verify the authenticity of the key.

The key management in wired network solution is based on public key infrastructure (PKI) where CA (certificate authority) releases certificates binding the public keys to specific users/nodes. In adverse conditions node is fallen into the wrong hands or the node is disqualified, then certificate should be revoked. Revoked certificates are added to the certificate revocation list (CRL). The CA (certificate authority) signature guarantees the authenticity of certificates and CRLs. Under certain assumption centralized trusted entity may not be considered for ad hoc networks where overall availability cannot be guaranteed all the time. The proposed authentication schemes for ad hoc networks involved certificate-based PKI. The key-management in these schemes advocates various ways to distribute the CA (certificate authority) functionality.

The instinctive approach of naive CA (certificate authority) to replicate key is not considered good enough. The risk of getting it compromised is high due to more nodes holding the private key issued by CA. A new type of public key system is introduced by Identity-based public key schemes [8]. Such kind of schemes permit user identities (e.g., E-mail or IP addresses) to be employed as public keys, and make certificates to meet out the requirement. In spite of that a trusted entity is mandatory in order to generate and share out the private keys corresponding to the different identities. The trusted entity is desired for revocation. The trusted entity may sign a list of withdrawn identities. As with conventional public key systems, it has been suggested to spread the trusted entity over more nodes. Symmetric systems aim at distributing one or more shared secret through secure channels. Many of the symmetric key management systems, for ad hoc networks, found in the literature are intended for Wireless Sensor Networks (WSNs). The sensor node has very limited power, memory, and computational resources, therefore symmetric systems may thus be the only option. WSNs have certain amount of infrastructure and are thus not truly ad hoc networks. A number of WSN schemes have been included in order to evaluate their applicability in traditional MANETs.

3. SURVEY OF RELATED WORK.

Unlike wired networks, fixed infrastructure may not be considered in a MANETs. Therefore, to make the certificate based authentication protocol suitable for MANETs is quit challenging task. For example, creation, distribution, renewal and revocation of certificates are done by certificate Authority (CA) which acts as a base for this system. It is difficult to consider the presence of centralized authority (CA) in mobile ad hoc networks due to factors likes node randomness, frequent link failures, wireless limited medium. There are three phases in certificate based authentication. During the "bootstrapping phase,CA (certifying authority) issues a certificate to the nodes. CA created a certificate using name of organization, IP address, and its public key. During the second phase due to the expiration, the certification is renewed". In the third phase the CA revokes the certificate due the compromise of the private key or the issuer believes that the user key binding is not valid. In MANETs several authentication mechanisms has been introduced to deal with the unique challenge of adopting certificate based authentication in MANETs. This paper provides twofold contribution; first, evaluate the requirements of secure distributed authentication system in MANET. Secondly, study of some exiting authentication schemes and their comparison in the context of distributed authentication. Beside of this, there are performance analysis metrics to evaluate the certificate based authentication schemes.

3.1 Self organized public key management

Capkun, buttyan and hubaux formulated the certificate graph [2] which is similar to PGP (pretty good Privacy) certificates [10]. It also defines a graph G (VE) where V and E stand for the set of vertices and set of edges, respectively. Public key represented by vertices and certificate represented by the edges of the graph. In the given diagram, an edge is directed from vertex ka to kb which represents the certificate issued by a to **b** by **a**'s signing **b**'s public key k_b with its own private key.

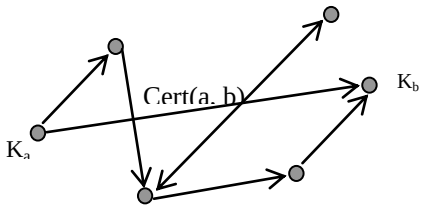


Figure 2: $K_a \rightarrow K_b$, certificate issued to b by a

Thus, for **b** CA (certificate Authority) is the **a.** only valid certificates of the whole network is contained by G. Here, each node maintains two repositories. These repositories consist of subset of expired certificates and updated certificate respectively. The use of two repositories provides a good assess of certificate graph for node authentication but incur high cost. If **a** wants to verify the authenticity of the public key of **b** at that time the update certificates repository graph of **a** and **b** are merged to find a directed path in resultant graph. To authenticate **b**, **a** chain of certificates on that path is used.

The node may merge its updated and non-updated certificate repositories to find expired certificates, if no path is found. When the expired certificates are found in a path it updates that and checks its correctness and performs authentication.

Public private key pairs are generated by every node at certificate creation phase. Whenever a new node requests for a new certification from its neighbor, the issuer verify the authenticity of the public key. Capkun et al [2] assumed that this may be done by a pre - exchange process of their keys over a secure channel. The certificate graphs are updated periodically by exchanging of hashes of the certificates with neighbor nodes. In this scheme, the maximums degree algorithm has been used to finding the path in the certificate graph. The paths with the highest number of certificate maximize the efficiency of the updated certification repository creation and updating.

This scheme does not describe the straight forward certificate renewal method as it is done when nodes gets the expired certificate in its non updated certificate repository. Capkun et al has suggested two methods for revocation of the certificates. In the first approach, the certificate is revoked automatically whenever the expiration time is encountered. In the second method, the straight forward revocation statement is issued by the issuer to the target node with the fact that it has no longer valid user-key. This is sent to the nodes that request the issuer for updates of the certificate for the target node.

By using the certificate, this scheme provides the self organized public key management. To maintain the expensive tables and to renegotiate one node with other nodes as each time a node move from one locality to another are the drawbacks of this scheme. However, the advantage of this mechanism is in its fully self-organized management of public keys.

3.2 Threshold and identity-based key management

Hongmei, Annindo and Dharma[3] have proposed authentication approach on recently developed concepts of identity-based cryptography [14] and threshold secret sharing [15]. It has some dissimilarities with other proposed schemes [16] [17] with respect to key generation and distribution. It does not consider the presence of CA to develop a trust relationship among nodes. In this scheme the key generation and distribution services are executed in a self organized manner.

In the initial phase, each node randomly chooses a secret and polynomial function of degree k-1.All the nodes jointly create a master key <PK, SK> public/private key pair. The key generation components produce master public/private key pair in such a way that all the nodes in the network must be familiar with the master PK, whereas The master private key SK is shared by nodes who jointly create it in a **(k, n)** threshold fashion**.** The all **k** nodes hold a unique secret share of the master private key SK, and no one is able to reconstruct the master private key based on its own information. The key generation service is provided to all the nodes in the network.In this scheme, before utilizing any network service, the node within the network must obtain its own private key corresponding to its identity and use this key to register itself in the network. To get the personal private key the node requests private key generation (PKG) service from at least its k neighboring nodes. Every node in network which have master key share can be the PKG service node. The identity works as the node's public key. After that, each node in the network publishes P and S_iP where S_i is secrete of corresponding node and P is a common parameter use in ID base scheme Then after, master public key is created by adding the SiP component of each node in the network. In this scheme, PKG issues the keys only once for a particular node, so that an adversary cannot duplicate the existing identity in the network.

In this scheme, when a new node joins a network, it requests to its share of the master key and master public key. In order to this it needs to publish all the required information likes identity, self-generated temporary public key to its k neighboring nodes. Each node in the coalition jointly verifies the validity of new node. After the successful verification the masker key generation process is started again. Then after, node gets its master private key share and ready to provide PKG service to other new joining nodes. The PKG service major cause for more communication overhead in network initialization phase. The main advantage of this scheme is that, there is no need for certificate generation, propagation, and storage because the public/private key pair is generated by the PKG service nodes.

Besides that, the scheme not only enhances the security but also reduce the resource consumption and communication overhead.

3.3 Dynamic key-scheduling and authentication scheme for distributed wireless network

T. Reddy [4] introduced a scheme which is based on fully self-monitored key management system. In this scheme node itself performs many tasks like key creation, store and revoke since it does not relies on trusted third party or fixed server. Therefore, fully self-monitored key management system allow nodes to generate their key pairs, issue certificates, and perform authentication without consideration of network partitions and centralized services. This scheme has adopted various security mechanisms to ensure the secure routing in the network. The certificate is a data structure where key is bound to be an identity (and possibly to some other attributes) by the digital signature of the issuer of the certificate.

In this scheme, nodes have responsibilities for the storage and distribution of certificate. Each certificate contains two attributes one is issuing time and other is expiration time. These two factors are used to verify the validity of the certificate. The issuer of the certificate issues an updated version of the same certificate with an extended expiration time. The self-organizing concept includes two phase

1. Key Distribution /Initialization
2. Authentication.

In the key Initialization phase, each node creates a key pair and certificate. In key distribution where each node find its nearest (one hop) neighbors and broadcasts it's key to all of its neighbors. Therefore, each node has received a set of key from its neighbor. Upon receiving a set of keys, node issues a certificate comprising the sending node id and key along with its own key which show the trust on sender identity.In authentication phase, the two nodes must exchange certificates before starting communication. The certificate consists id's and keys of both nodes engage in exchange of certificate. As discussed earlier, every node individually maintains a repository table.The network has a beacon period during which network operations such as initialization of network as well as communication are carried out. Any change in the network, due to dynamic nature of MANETs, may not be considered till the completion of beacon period. Once the beacon period is completed, every node again tries to find out its neighbors. In this process, node may encounter the old neighbors or the node may encounter some new nodes. Upon receiving certificates, node checks the certificate within its back up repository table. If it does not find the match, the newly received certificate is

ignored. Otherwise it will be stored in updated repository of the node. The advantage of this scheme is that it produces low communication overhead due to the construction of local repository. This scheme may allow the partition of network so that nodes may communicate with only a subset of other nodes. Authentication is still possible in this situation. Each certificate is issued with its issuing and expiration time, so before expiration of certificate, its issuer issues a update version of same certificate with extended expiration time. Each node periodically issues certificate updates, until the owner considers that the node identity contained in these certificates are correct. Node can revoke its certificate if it believes that its private has been compromised. Similarly node can revoke the issued certificate if it experiences some disturbance in key binding.

3.4 Trust- and Clustering-Based Authentications

Ngai et al [5] has described a trust and network model to improve network's security and efficiency of public key certificate. This scheme presumes that, the network model is clustered by clustering algorithms. They realize the importance of such algorithms to enhance the security and efficiency of the network. In this scheme, they introduce web of trust model, like PGP(pretty good privacy)[10].Each node keep a list of trust values for another nodes in the network. The trust values considered to be continuous values between 0 and 1. A trust relationship between two nodes in the same group is a direct trust and is different group is a recommendation trust. For monitoring the behavior of the nodes, the nodes are supposed to be associated with some detecting component like watchdog, so they can determine which nodes are trustworthy within the group.

In this scheme, each node is supposed to keep trust table for storing the trust values and public keys of the nodes they know. When node wishes to authenticate a another node in different cluster, it has to communicate with several other introducing nodes of that cluster. It is assumed that a cluster contains a public key management.The Introducing nodes are sorted on the basis of trust values. There are two nodes s and t. They do not have trust relationship due to long distance therefore node s has to reach t via the recommendation of an introducer. The trust value between s and introducer is considered as recommended trust. The trust value between s and t is calculated by summation of the trust values of its introducing node with trust values of the introducing nodes which appear on the path to the target nodes. There is no provision of renewal and revocation of the certificate .This scheme discovers and isolates malicious nodes. It is the main strength of this scheme. Its disadvantage is that the storage of the trust value is both memory & time consuming.

4. BASIC REQUIREMENTS FOR CERTIFICATE BASED AUTHENTICATION SCHEMES

The requirements for certificate-based authentication scheme in MANETs to be considered as secure and effective have been identified.

A.1 *Authentication function*: The distribution of the certificates amongst a set of nodes is one of the primary requirements of the certificate based mechanism in the ad hoc network. This process may be affected by the issues such as node instability, limited wireless medium and frequent link failures. It is impossible to comprise a fixed centralized authority (CA) in the ad hoc networks. The scenario, where presence of centralized authority (CA) is valid even then the process of the certificates distribution may not be performed smoothly. Because, centralized server could become a single point of failure in a networks and require high security. For instant, consider a scenario of the battle field, where the troops are spread out in a large area. In such a case, presence of central server might not be feasible. If server is attacked by the enemy, then this would bring down the whole network.

A.2 *Resource constrictions*: The authentication protocols must be aware about the resources because nodes in ad hoc network run on batteries with high power consumption and low memory capacity. Therefore, space and time complexity of authentication method must be low. The symmetric key based cryptographic techniques incur less resource consumption as compare to public key method. In an ad hoc network the practical deployment of such techniques are prevented by the issues such as distribution of symmetric keys. The authentication protocols in ad hoc networks which are using public key method (Resource intensive) for certificate creation should be efficient with respect to less resources consumption.

A.3 *Efficient certificate management*: In case of wired networks, the extensive study has been done regarding distribution of public key and management of certificate[1]. However, to adopt the same approach in MANETs is quite challenging issue, due to managing the certificates. This issue is further discussed in sections 4. Most of the current mechanism does not have strong certificate revocation scheme.

A.4. *Heterogeneous certification*: The certifying authorities (CA) not only in wired networks but also in ad hoc network could be heterogeneous. In this case, nodes can authenticate each other, even though they are associating with different "domains". In that case, there should be some kind of trust alliance among the nodes. This trust relationship can be achieved through certificate chaining in wired network.

A.5 Pre-authentication mechanism: The pre-authentication is the process to build essential trust between nodes before the actual certificate creation and distribution. It is pretty crucial in MANETs, though this is not a part of the certificate authentication process itself. It is mandatory that nodes have prior trust between each other to satisfy R1.The renewal of certificate and later Mutual authentication may not be possible without this establishment.

location limited channel. A more user friendly approach has been discussed by balfanz [9].

4.1 Comparisons of the different mechanisms

Table 1 compares the four authentication mechanisms with respect to the requirements. The requirement R.5 is not an inherent part of the certificate mechanism itself so it is not considered in comparison table 4.1.

Table4.1: Comparison of Certificate-based Authentications

Requirements	*"Threshold and Identity-based Key Management* Hongmei[3]"	*"Self Organized Public Key Management – Capkun*[2]"	*"Trust- and Clustering-Based Authentication Ngai*[5]"	*"DynamicKey-Scheduling and Authentication Scheme for Distributed Wireless Network – T.Reddy*[4]"
A.1. Nature of Authentication functions	Totally distributed and scales well to large networks	Every node creates certificate itself and act as a CA.	Distributed and self organized since every node acts as a CA	self organized since every node acts as a CA
A.2. Resource constrictions	Master key pair computed collaboratively by the nodes in the network. In this key generation process a polynomial function is used. So, This process is resource-intensive and time consuming.	Each node keeps two certificate repositories, which incurs a high overhead.	The maintenance of trust tables and the monitoring components are memory intensive.	Each node maintains two certificate repositories, which incurs high overhead.
A.3Efficient *certificate management* A.3.(a)Certificate Creation	Requires at least k neighbors which might be a bottleneck. Use Identity as public key	Self–signed certificates, and hence more robust than a shared key based mechanism	Across nodes creation is based on trust values. The existence of introducing nodes may not be true at all times.	Node self generated its key pair.
A.3.(b) Certificate Renewal	Same as issuance	No explicit mechanism discussed	Not discussed.	Issuer issues an updated version of the same certificate with an extended expiration time.
A.3.(c) Certificate Revocation	No explicit mechanism discussed	Using explicitly revocation methods a certificate can be revoked.This approach produces delay between far-away nodes in the network.	Not discussed.	Each node maintain a update repository, hence it is memory intensive.
A.4. Heterogeneous certification	Not implemented.	Not implemented.	Implemented using trust graph	Not implemented.

5. METRICS FOR PERFORMANCE EVALUATION

The following metrics have been identified, based on which the authentication mechanisms can be evaluated.

a)Certification Hit-Ratio: It measures the ratio of the number of successful certification services including issuance, NC_{ISS} and renewal NC_{REN} to the total no. of requests for such services (NCTOT-ISS and NCTOT-REN) respectively. If H_{REN} is the successful certification renewal ratio and H_{ISS} is the successful certificate issuance ratio. Then their values are:

$$H_{REN} = \frac{NC_{REN}}{NC_{TOT-REN}} \quad H_{ISS} = \frac{NC_{ISS}}{NC_{TOT-ISS}}$$

Here, NC_{REN} and NC_{ISS} are the respective total number of certificate renewed and issued, and $NC_{TOT\text{-}REN}$ and $NC_{TOT\text{-}ISS}$ the respective number of requests for certificate issuance and renewal.

b) Establishment time (et): Time taken to issue valid certificated for all the nodes is measured in it. Therefore, the value of et can be calculated as the time difference between when all the nodes are issued valued certificates & the stating time when this process begins. The no. of malicious nodes, the algorithms used for key generation and distribution are the factors on which the setting time depends. The effective mechanism of pre-authentication will decrease the establishment time.

c) Through Put (T): measures the number of certification services executed within time T.

$$T_{cert} = \frac{N_{cert}}{T_{\text{int}}}$$

Here, Ncert is the total number of certification services and Tint is the simulation time. Frequent certificate insurance and renewal process are expected because of dynamic nature of network topology. For the public key mechanism, costly computation has to be carried out when every time node want to create or renew its certificate.

d)Average Certification Delay (Tavg): It is summation of difference of certificate service reply (CS Rep) and certificate service request(CSReq) and averaged over the simulation time.

$$Tavg = \frac{\sum_{i=1}^{n} (CS\,\mathrm{Re}\,p_i - CS\,\mathrm{Re}\,q_i)}{T_{\mathrm{int}}}$$

.

Table 2: Parameters for the battlefield scenario

Dimensions	1670*970
Mobility Model	Reference Point Group Mobility Model (RPGM)
Min. speed	1 m/s
Max. speed	2 m/s
Number of node	50
Pause time	50 sec
Maximum distance to group center	50m

This value is used to estimate the efficiency of the algorithm, and mainly depends on the time complexity of the algorithm.

6. PARAMETERS FOR DEFINING THE SCENARIOS

The mobility model is designed to describe the movement pattern of mobile nodes, and how their location, velocity and acceleration change over time. They can be mainly classified as group mobility and models entity mobility models. Camp et al. has given a broader classification of these models [11]. The most commonly used mobility model is the RWM (Random Waypoint Model) which uses pause times and the random changes in destination and speed. In spite of this, the Random Waypoint mobility model is not sufficient to represent the some realistic scenarios of MANET deployment, such as battlefield, rescue operation, etc. Further, this model has failed to offer "steady-state" over a long simulation period [12]. Thus, the selection of mobility models with respect to certificate-based authentication mechanism should be done carefully. Following aspect should be looked into advance.

This section briefly discusses the realistic simulation "scenarios", in order to understand the effectiveness of these mechanisms. We first need to describe some parameters to better understand the scenario.

1. *Node Density:* it varies according to a particular scenario. For example, disaster recovery scenario might have a low density as the nodes are spread out over a wide area whereas event coverage scenario may have a high density of nodes.

2. *2. Traffic rates: This varies* according to the node congestion, linkage failures and mobility. While defining the scenario the sources and traffic type (for example, CBR, TCP or UDP) must also be taken into account. The traffic type which is normally used is Constant Bit Rate (CBR). The size and packet rate for a realistic scenario could be 512 bytes and 4 packets/sec respectively.

6.1 Experimental Setup

For the scenario-based experiments, we used the ns-2 simulator which is available as an open source distribution [**13**]. Specifically, the ns-2.28 version is used on a Cygwin environment. CMU's wireless extension to the ns-2 simulator is used, which is based on a two-ray ground reflection model. The radio model corresponds to the 802.11 Waveland, operating at a maximum air-link rate of 2 Mbps. The traffic pattern is generated using "code.tcl" script. The CBR traffic is generated with 512 byte application data payload size. The simulation is run for 500 sec. To analyze the performance of SAODV The battlefield scenario is chosen. In this scenario 50 nodes are distributed over the simulation area. The parameters for this mobility model are listed in table 4.2 .The total number of nodes is 50, while each node stays at a maximum of 50 meters from the group leader. The maximum speed of the nodes is taken as 2 m/s (which may depict military motor vehicle) and minimum speed as 1 m/s (movement of soldiers).

6.2 Metrics for Performance Evaluations

The following metrics are used for performance evaluation

Packet Delivery Fraction (PDF): This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation.

$$PDF = \frac{numberOf\,\mathrm{Re}\,ceivedPackets}{numberOfSentPackets}$$

A higher value of PDF specifies that the packets are being delivered to higher layer with high rate and it is a good sign of protocol performance.

Normalized Routing Load (NRL): This is the ratio between the no. of routing packets transmitted to the number of packets actually received (thus accounting for any dropped packets).

$$NRL = \frac{numberOfRoutingPacketsSent}{numberOfDataPackets\,\mathrm{Re}\,ceived}$$

This metric is used to evaluate the efficiency of routing protocol. It gives idea of how well the protocol maintains the routing information updated. The higher value of NRL indicates the higher the overhead of routing packets and hence ,lower the efficiency of the protocol.

Average end to end delay (AED) : This is defined as the average delay in transmission of a packet between two nodes and is calculated as follows-

$$AED = \frac{\sum_{i=0}^{n} (timePacket\,\mathrm{Re}\,ceived_i - timePacketSent_i)}{TotalNumberofPackets\,\mathrm{Re}\,ceived}$$

This metric is used to find the congestion in the network. A higher value of end-to-end delay reflects that network is congested and hence the routing protocol doesn't perform well.

6.3 Result

The pause times are varied from 0 to 50 sec for the scenario. The impact of scenario for three routing protocols (SAODV, DSDV, DSR) is studied on the three metrics i.e Packet delivery fraction, end to end normalize routing load.

6.3.1 Impact on the Packet Delivery Fraction (PDF)

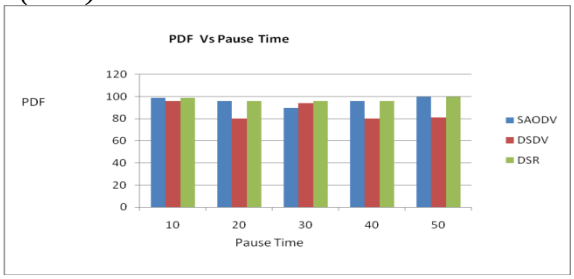


Figure: 1.2 PDF Vs Pause Time for battlefield scenario.

It is found that for the battlefield scenario, SAODV perform better as compare to DSDV and DSR protocols in terms of packet delivery fraction for higher pause times as shown in figure 5.3. This can be attributed to the fact that DSDV uses the *weighted settling delay* to reduce the number of routing table updates, For higher pause times (greater than 40 sec), the PDF becomes stable for all three routing protocols. Therefore, it may be assumed that nodes are almost static. At the higher pause time, the SAODV and DSR routing protocols obtain almost 100% PDF.

6.3.2 Impact on the Normalized Routing Load (NRL)

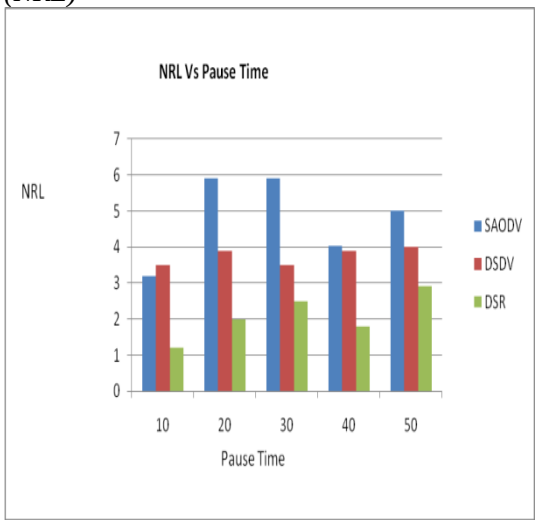


Figure-1.3 NRL Vs Pause time for battlefield scenario.

In all pause time interval, SAODV shows higher routing overhead than DSR and DSDV. DSR obtains least overhead because it is a reactive protocol and hence advertises routes only when required as opposed to the periodic routing updates in DSDV and SAODV. The performances of DSR emphasize the fact that a reactive routing protocol is more adaptive to the mobility of nodes than proactive routing protocol.

6.3.3 Impact on the Average End-to-End Delay (AED)

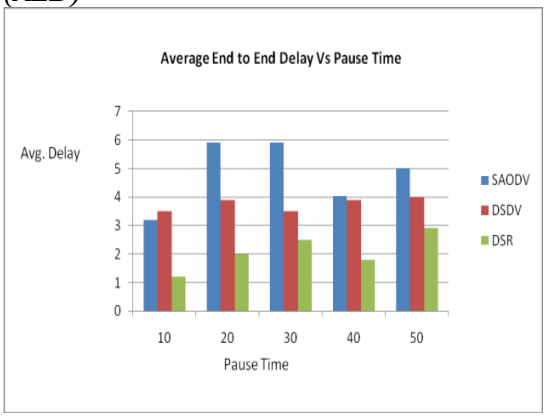
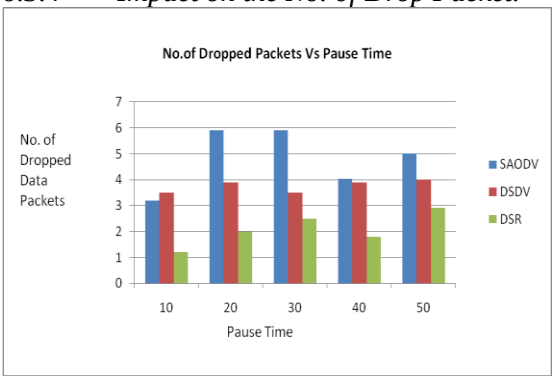


Figure: 1.4 AED Vs Pause Time for battlefield

scenario exhibits a higher delay than DSDV and DSR. This is understandable, since the computation of hash functions for authenticating the routes adds to the processing overhead at each node. Further, we find that as the mobility increases, the average end-to-end delay increases.

6.3.4 Impact on the No. of Drop Packet.



SAODV shows higher dropped packets as compare to DSR and DSDV.since, SAODV has security mechanism to detect the malicious node. This experiment is done in the presence of six malicious nodes. This security mechanism provides security against impersonation, modification & non-repudiation.

7. SUMMARY AND FUTURE WORK

The significance of successful authentication is crucial for assuring security and effective operation of the supported application, especially in distributed field applications where mobile nodes are spread over a large geographical area.

Several certificate-based authentication mechanisms have been proposed for MANETs. Here, some of these mechanisms have been discussed with their merits and demerits. This paper identifies the requirements of certificate based authentication schemes in MANETs. The discussed schemes have been compared to the listed requirements.

Other than this ,the experiments is carried out using routing protocols– DSDV, DSR and SAODV. The set of scenarios can be used for simulation study such as battlefield, rescue operation. In this paper, battlefield scenario is used to derive the result. On one hand, the battlefield scenario requires high reliability and high security, along with high overall performance, whereas the nodes in this scenario have to save power due to limited processing capability.

Other than its security aspect, SAODV is unsuitable for the battlefield scenario mainly because a high value of NRL indicates higher network congestion. Besides, higher value of AED implies not only lesser throughput but also demands greater processing power for the nodes. Further, the proactive nature of SAODV causes more power consumption at each node due to more number of routing advertisements. If security is not an issue, DSR would be an ideal choice for this scenario.

8. REFERENCES

[1] [1] Internet X.509 Public Key Infrastructure Certificate and CRL Profile - RFC 2459.

[2] [2] S. Capkun, L. Buttyan and J-P Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc

[3] Networks ", IEEE Transactions on Mobile Computing, Vol. 2, No. 1, Jan-Mar 2003, pp. 52-64Hongmei Deng, Anindo Mukherjee, and Dharma P. “Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks ", in the Proceedings of IEEE Information Technology: Coding and Computing, 2004.

[4] T.Surya Prakash Reddy, T. Sunil Kumar Reddy. " Dynamic Key-Scheduling and Authentication Scheme for Distributed Wireless Network. Int. J. Advanced Networking and Applications Volume: 02 Issue: 01 Pages: 464-469 (2010)

[5] Edith C. H. Ngai and Michael R. Lyu. "Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks", 24th International Conference on Distributed Computing Systems Workshops - W4: MDC (ICDCSW'04), Hachioji, Tokyo, Japan, 3/23-24, 2004.

[6] L. Zhou and Z. Haas. "Securing Ad Hoc Networks", IEEE Network magazine, special issue on networking security, Vol. 13, No. 6, November/December 1999.

[7] Matei Ciobanu Morogan, Sead Muftic. "Certificate Management in Ad Hoc Networks", 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), January 27 - 31, 2003, pp. 337.

[8] F. Stajano and R. J. Anderson. "The resurrecting duckling: Security issues for ad-hoc wireless networks" In 7th Security Protocols Workshop, volume 1796 of Lecture Notes in Computer Science, Cambridge, United Kingdom, 1999. Springer-Verlag, Berlin Germany.

[9] Dirk Balfanz, D. K. Smetters, Paul Stewart and H. Chi Wong: "Talking To Strangers: Authentication in Ad-Hoc Wireless Networks", Symposium on Network and Distributed Systems Security (NDSS'02), Xerox Palo Alto Research Center, Palo Alto, USA, 2002.

[10] P. Zimmerman. The Official PGP Users guide, MIT Press, 1995, ISBN 0-262-74017-6.

[11] T. Camp, J. Boleng, and V. Davies. "A Survey of Mobility Models for Ad Hoc Network Research", in Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, vol. 2, no. 5, 2002.

[12] J. Yoon, M. Liu, and B. Noble. "Random waypoint considered harmful," in Proc. of IEEE INFOCOM '03, vol. 2, March 2003, pp. 1312—1321.

[13] K. Fall and K. Varadhan, The NS Manual, The VINT Project, UC Berkeley, January 2002.

[14] A. Shamir, "Identity based Cryptosystems and Signatures Schemes," Proceedings o f the Advances in Cryptology, 1984.

[15] A. Shamir, "How to Share a Secret," Communications of the ACM, Vol. 22, No. 11, pp. 612-613, November 1979.

[16] L. Zhou and Z. J. Hass,"Securing Ad Hoc Networks," IEEE Networks Special Issue on Network Security, November/December, 1999.

[17] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A Secure Routing Protocol for Ad Hoc Networks," Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.

[18] D. Bonh and M. Franklin, "Identity-Based Encryption from Weil Pairing," Advances in Cryptology, CRYPTO 2001, Lecture Notes in Computer Science, Vol. 2139, pp. 213-229, Springer Verlag, 2001.

[19] ANNE MARIE HEGLAND, ELI WINJUM, STIG F. MJØLSNES, CHUNMING RONG IEEE Communications Surveys & Tutorials • 3rd Quarter 2006