**Indonesian Journal of Electrical Engineering and Computer Science**
Vol. 10, No. 2, May 2018, pp. 654~663
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i2.pp654-663 

# A Novel Approach Certificate Revocation in MANET Using Fuzzy logic

**Jayanthi. E, Mohammed Ali Hussain**
Department Computer science and Engineering, KL University, Guntur Dist., A.P., India

**Article Info**

***Article history:***

Received Nov 6, 2017
Revised Jan 25, 2018
Accepted Feb 19, 2018

***Keywords:***

CA
CMP
CRL
CRS
ECDSA
EDDEEC
LEACH
MANET
OSCP
PKI

**ABSTRACT**

Due to the advent developments in the Information and Communication Technology (ICT) based environment, Mobile ad hoc networks (MANETs) have fascinated much concentration because of their mobility and easy deployment. At the same time, their wireless and vibrant features make them susceptible to wide range of types of security attacks when compared to the traditional wired networks. The prime challenge is to assure security in the network components and services. To work out the challenge, novel security measures are put forward for effective and secured communication. In our proposed work, we discuss the need for Security in MANET, focusing on certificate revocation. Providing security is challenging tasks due to its key features. Different authentication techniques, Digital certificate and components of Public Key Infrastructure are also discussed. The certificate revocation is a challenging task in MANETs due to absence of centralized repositories and trusted authorities. The different methods of certificate revocation using cluster based mechanism is analyzed and compared. The principle, advantages and disadvantages of certificate revocation are also compared. And the novel Certificate revocation techniques using fuzzy is discussed with reduced overhead.



***Corresponding Author:***

Manisha R. Dhage,
Department of Computer Engineering,
K.L. University,
Guntur Dist., A.P., India
Email: jntkamal@yahoo.com

## 1. INTRODUCTION

The MANET (Mobile Adhoc NETwork) comprises of dynamic network topology, limited bandwidth, energy constrained nodes and very limited physical security. MANETs are developed mainly for networks, in which users can join and leave the network without any centralized control. Security is the important prerequisite for any wireless networks. Mobile Adhoc networks are more vulnerable to attacks than the wired networks. Hence it is a challenging research topic. The intruders can carry out active and passive attack due to exposed nature of the MANET. The basic security requirements can be violated, by leaking secret information or by impersonating nodes. The security requirements of wireless Mobile Adhoc NETworks are access control, Authentication, Non repudiation, confidentiality, integrity and availability. Mobile Adhoc NETworks is useful in places where infrastructure is not available and is impossible to install. The applications of temporary networks are required in military applications such as communications for soldiers, tanks and planes. In Civilian environments for taxi cab networks, meeting rooms, stadiums, aircrafts etc. For Emergency operation such as search and rescue, monitoring, firefighting, rescue and finally for personal area networking using cell phone, laptop, ear/head phone, wrist watch. Another major application is in the area of disaster and emergency. For, interconnection of sensors in military and commercial places, of all the above discussed applications military or any networks where sensitive communication is involved is

likely in need of basic security requirements like authentications and confidentiality. Authentication is the foundation of safe and secure communication.

The security issues relating to authentication are limited resources, decentralized and infrastructure less network and high mobility. The above issues are challenging factors for creating a secure adhoc network, where authentication needs to done followed by other basic security requirements as stated above. Also the main characteristics of Mobile Adhoc NETworks [1] are to provide Authentication using less computation and communication overhead. Above all these constraints the CPU resources availability including battery power are minimum. To provide authentication in such a constrained network is the challenging task. The security techniques for authentication are proved by (i) Symmetric cryptography (ii) Asymmetric cryptography (iii) collaborative mechanism. The advantage of Symmetric cryptography is the negligible computation and communication overhead. However this method is used only for small networks, and if the shared secret key is compromised then the entire network will be compromised. Hence these problems make symmetric key cryptography unsuitable for MANETS. This can be evaded by using Asymmetric key cryptography. Asymmetric key based cryptosystems provide basic security requirement such as authentication and non-repudiation and easier key distribution, this could be an enhanced choice for the MANETs. The third mechanism is Collaborative mechanism also known as threshold cryptography used in distributing the role of certificate authority among the participating nodes. But consequently the communication overhead is higher as it takes advantages of both symmetric and asymmetric mechanism.

### 1.1. Digital Certificates

In [2] a digital certificate is electronic passport which is used to exchange information securely over internet with the help of Public Key Infrastructure (PKI). The digital certificate is also known as public key certificate. Components of PKI: In infrastructure networks, a trusted third party, known as Certification Authority (CA) distribute certificate to users which contains users public key and an identity. There by secure communication is provided among users and it ensure security requirements like authentication, confidentiality and integrity. In earlier Public Key Infrastructure (PKI), a Registration Authority (RA) collects and analyzes all requests before sending them to a CA to certify, issue revoke or renew user's digital certificate. In Mobile Ad hoc Networks (MANETs), to avoid single point of failure apart for mobility and other issue a decentralized certificate authority approach is utilized. A cluster head is elected per cluster by the cluster members. The cluster head plays the role of Certificate authority. We safely distribute functionality of the certificate authority to nodes in the network without compromising the security of its private key by using the following approaches: Partially Distributed Certificate Authorities, Fully Distributed Certificate Authorities, Certificate Chaining, Mobility Based Certificate Authorities, Cluster Based Certificate Authorities, and Identity Based Certificate Authorities. Wireless devices are prone to technical limitations like less powerful CPU, low memory, less battery power, reduced display and input devices as compared to devices in wired network.

a) Mobile devices lacks processing and computing abilities of PKI services such as key generation, digital signature generation/verification, certificate validation, Certificate Revocation and CRL. The processing of CMP in the mobile devices, and downloading CRL required for certificate verification becomes very hard because the technical limitations of wireless environment
b) PKI in wireless environment, same security level as wired PKI. The nodes in MANET have limited resources in terms of processor and memory; hence magnitude of the certificate and the validation practice needs to be optimum. WPKI services needs cost be optimized by adapting more efficient cryptography and data communication techniques for Mobile Adhoc Networks.
c) Optimal Digital Signature: For optimal Digital Signature the main algorithms used are ECDSA (Public-Key Algorithm), DES (Symmetric-Key Algorithm). ECDSA has less overhead as compared to DES for MANET. Basic task is to reduce the size of the certificate by deleting unwanted and unused fields from the certificate. By doing so optimal certificate can be generated.
d) Optimal Certificate Request and Management Protocol: The MANET nodes demand for certificate from the Certificate Authority. The Certificate Authority then issues the certificate to the requested nodes after validating the node. The above procedure is done using certificate request protocol. The mandatory fields are filled in the certificate's request message format and sent very securely to the CA. To conclude the above task wireless, certificate management protocol is utilized in an optimal way.
e) Optimal Validation Certificate validation is difficult wireless networks than in conventional network. In [3] the application of different mechanisms for certificate validation in MANETs and present a cooperative mechanism for certificate validation suitable for MANETs is discussed. Also discuss to decrease the complexity of certificate validation, with the size of the certificate reduced. Each public key infrastructure needs an efficient certificate status validation method to exclude the

revoked certificates from network. Present a novel certificate validation scheme called Enhanced-ADOPT with novel certificate status information. The OCSP response messages are modified to carry information about the accusations provided against the certificate and this extra security information helps the client nodes to modify the OCSP results accurately. Thus client node can alleviate the certificate status information discrepancy problem with lesser overheads and provide effective certificate status validations in MANET. Based on the validity period of the nodes, the nodes are revoked if validity period is reduced to zero. However, certificate validation is a vital task as the mobile node are required to check the validity of certificates for communication in real-time.

### 1.2. Attacks in MANET

Explaining An approach while considering MANET design is to have an observation on threats, attacks and vulnerabilities. The threats Attacks in MANET are classified as passive attack and active attack like the wired counter networks. Various types of active and passive attacks are discussed. These attacks can be classified into collaborative and non-collaborative attacks. In Non-collaborative attack only one node plays a major role in attacking the network. Collaborative attacks [4] occur when more than one attacker disturb a target network. There are different types of collaborative attacks like Denial-of-Messages (DoM) attacks, Black hole attacks, Wormhole attack, Replication attacks, Sybil attacks, Rushing attacks, Malicious flooding . All of the above attack has defensive mechanism. Different machine learning techniques and digital signal processing techniques can be adopted to detect and protect against attacks in MANET.

### 1.3. Certificate Revocation in MANET

In [5] proposes a novel criterion based on risk involved to check and properly evaluate cached status of the data that is much accurate, appropriate and absolute than time as it takes into account the wireless certificate revocation in MANET. In this Certificate Revocation is process in MANET similar to wired network, where a node can revoke a certificate that it has issued, if the revoking node believes in that certificate is no longer valid or if a node's private key is compromised, and to revoke its public key. There are two types of certificate revocation technique, explicit and implicit revocation technique. The explicit revocation scheme, certificate owner (Certificate Authority) possesses a proof of non-revoked certificate. And the remaining certificates are revoked. Example of this type is Certificate Revocation System (CRS). The disadvantage is the process involved like generation, maintenance and distribution of various secure data structure. The implicit revocation scheme is constructed based on the expiration time of the certificates. Certificate is implicitly revoked on expiry. Hence, it is very essential to correctly assign the length of validity time. This enables users to perform authentication with a higher confidence in the validity of the certificates, also in the rightness of the user-key bindings enclosed in the certificates because of their limited validity period. If the owner's the private key is compromised, then the corresponding public key is revoked by notifying the users that issued certificates to her. Certificates are revoked to isolate malicious node from Mobile Adhoc Network. In wireless certificate revocation is difficult and challenging because the nodes are not stationary. And certificate revocation is a major research area in MANET. Whereas the certificate revocation is a challenging task in MANETs and also this method of certificate revocation is not suitable for MANETs due to the unavailability of centralized and trusted authorities. The nodes in the MANET can be removed from the network based on identified attacks. The nodes can be eliminated from the networking by revoking the certificate.

There are different techniques of revoking certificates. For improved performance and reduced overheads Cluster based revocations in MANETS are used than traditional flat based system. Cluster-based Certificate Revocation has faster certificate revocation due to the clustering system. Clustering solves the problem of the false accusation. Another trust based threshold cryptography revocation scheme [6] for MANETs. Here the master private key is divided into n pieces according to a random polynomial. Each node in the proposed scheme is configured with a share ski of the CA private key SK, the node's public key PKI, and the CA public key PK before joining the network. The master private key is recovered by combining any threshold t pieces based on Lagrange interpolation. This improves the safety levels in MANETs. The proposed hop-by-hop certificate revocation scheme is based on both threshold cryptography and transitive trust between mobile nodes. Because of the decentralized nature of our proposed scheme, it enables a group of legitimate nodes to perform fast revocation of a nearby misbehaving node. The proposed scheme is highly robust in the mobility environment of MANETs. The advantages of the proposed scheme are justified through extensive simulations. To stop the attackers from further contributing in the network the certificate revocation is used. To eliminate the security threats, an efficient certificate revocation scheme is used to achieve a secure communication. Here, Vector-based trust mechanism (VBM) which nominates a CH based on the higher trust value computation with earliest bit vectors and Enhanced Certificate Revocation scheme (ECR) for discarding the authorization of the misbehaving nodes. Here the advantages are greater reliability,

minimum energy, and quicker revocation time compared to the existing mechanisms. Another challenge is revocation of certificate in timely manner. The above problem is solved using threshold based approach. This method is used to restore a node's accusation ability and also ensure proper normal nodes to accuse malicious nodes.

URSA-Ubiquitous and robust Access Control [7] where in the certificates are revoked based on votes from its neighbor. The certificates are revoked based on some threshold. But the disadvantage is determining the threshold. And also this scheme does not handle false accusation. Localized certificate revocation scheme does not have certificate authority; revocation is based on weighted accusation. If weighted sum from all the votes exceeds predefined threshold then certificate is revoked. But high communication overhead is experienced due to all the nodes participating in the election process. Also revocation time is comparatively high. Suicide for Common good is a new approach for credential revocation which results in quick revocation and less overhead. This is possible as only one accusation is taken. But, it does not deal with false accusation. CCRVC is a cluster based scheme. Certificate Authority manages the white list and the black list. Certificate can be revoked by only one neighbor. This scheme deals with false accusation but high communication overhead.

The Table 1 shows the comparison between voting based and non-voting based mechanism. Cluster based certificate revocation [8] which is the combination of voting based and non-voting based mechanism. This method proves to have good accuracy, rapid decision process, good reliability and security.

Table 1. Certificate Revocation Scheme

| Sr. No | Paramaters | Voting-Based Mechanism | Non-Voting-Based Mechanism | Cluster-based Certificate Revocation Scheme |
|---|---|---|---|---|
| 1. | Accuracy | Very High | Low | High |
| 2. | Decision process | Slow | Rapid | Rapid |
| 3. | Reliability | Less | Less | High |
| 4. | Security | Less | Less | High |

This paper provides an overview of a securing communication in network by using cluster-based certificate revocation method. Cluster-based certificate revocation has merits of both voting based and non-voting based mechanisms which revokes malicious certificate quickly. Problem of false accusation is also taken care by using Cluster-based certificate revocation mechanism. The threats categories that considered after the deployment of MANET are amateur adversary, professional adversary and well-funded adversary. And the process of wireless links creates the network prone to vulnerable attacks. In short MANET is vulnerable because of its characteristics like open medium and cooperative algorithms and also absence of centralized monitoring and line of defense. Secure communication between CA and CH is proposed with AODV Protocol for Routing. Exactly determining cause of packet loss in wireless network is a challenging task. One of the causes is by malicious nodes that perform the common attack called Black Hole attack [9]. A Secure & Efficient Audit Service Outsourcing method designed to prevent the fraudulence of prover [10]. An efficient mechanism on probabilistic queries and periodic verification is proposed to reduce the audit costs per verification and implement abnormal detection timely.

Fuzzy logic revocation [11] is based on fuzzy logic. The accused node is revoked based on fuzzy logic. With the use of fuzzy logic, malicious nodes are detected and removed from the network accurately by calculating Trust Values of a node at CA and CH. In [12] developed a multipath scheduler over the satellite networks supports load balancing methodologies based on optimum time-bandwidth in order to accommodate the burst of application traffics. Heterogenous network [13] has budding to improve network lifetime and also provide sophisticated quality network. Due to limited power battery will exhausted. Thus, energy efficient routing protocol needs to allocate the balance energy burden between the sensor nodes.

## 2. RESEARCH METHOD

Modules of Proposed Cluster-based Certificate Revocation Scheme using fuzzy logic are listed as follows:

a. Network formation with clusters
b. Creation of Certificate Authority (CA)
c. Certificate Distribution
d. Certificate Acquisition and Certificate Storing
e. Non-voting-based scheme with fuzzy logic
f. Detection of Malicious node

g. Revocation of Certificate from malicious node.

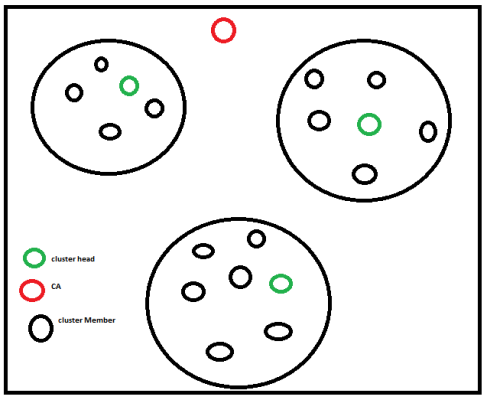


Figure 1. Cluster Formation in MANET

A Secure communication between CA and CH is proposed with AODV Protocol for Routing. Exactly determining cause of packet loss in wireless network is a challenging task. One of the causes is by malicious nodes that perform the common attack called Black Hole attack in the MANET. We have performed the attack and its detection method using routing protocol known as Ad Hoc Distance Vector (AODV) routing protocol. The neighboring nodes on hearing about the attack and informs about the malicious attack to CA.

Two scenarios can be generated

Scenario A: Random node claims another node as attacker (Fake).

Scenario B: Nodes actually detect a black hole attack (Attacker).

CA places the accuser node in BL and Accused node in WL. CA broadcasts the WL and BL lists to all CH. CH maintains all the information about the cluster members. All the cluster members calculate trust of one hop neighbor and share the value when cluster members request it. Trust of a node is based on the previous communication history. On hearing about accusation, CH Calculates the final Trust Value of both the accuser and accused node using fuzzy logic. Parameters like packet drop , Packet received, energy , jitter, trust , number of times the node has been accused , number of times the node accused another node, etc., are input parameters to Fuzzy system. Each parameter is assigned values between 0 and 1. Based on the value of the trust CA decides the trusted nodes and malicious nodes. Figure 2 shows how the nodes are classified as trusted and malicious nodes.

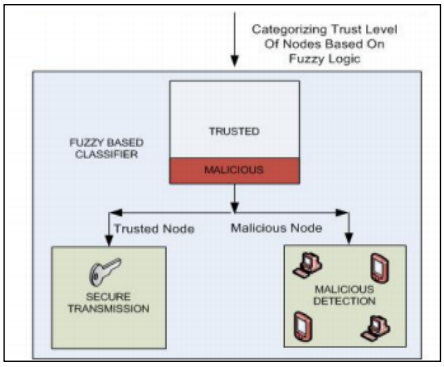


Figure 2. Security Frameworks

In the classical set, any parameters can only be categorized into one subset, LOW, MEDIUM or HIGH. But in fuzzy set shown in Figure 3, these boundaries become vague. This is fuzzy set union.

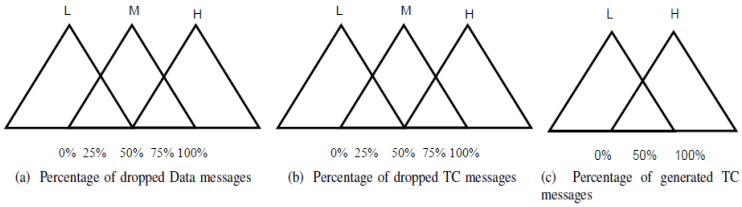


Figure 3. Input Parameters of Fuzzy-Based Scheme

Fuzzy mapping rules provide a functional mapping between input and output by using linguistic variables. The foundation of a fuzzy mapping rule is a fuzzy graph, which describes the relationship between the fuzzy input and the fuzzy output. The rules for fuzzy system and classes of fuzzy system are described in table 2 and table 3 respectively.

Table 2. Rules for the Proposed Fuzzy System

| Rule | %age of dropped data packets | %age of dropped TC messages | %age of generated TC messages | Trust |
|---|---|---|---|---|
| 1 | L | L | L | VH |
| 2 | L | M | H | VH |
| 3 | L | H | L | H |
| 4 | L | L | H | VVH |
| 5 | L | M | L | H |
| 6 | L | H | H | M |
| 7 | M | L | L | VH |
| 8 | M | M | H | H |
| 9 | M | H | L | M |
| 10 | M | L | H | VH |
| 11 | M | M | L | H |
| 12 | M | H | H | M |
| 13 | H | L | L | L |
| 14 | H | M | H | VL |
| 15 | H | H | L | VVL |
| 16 | H | L | H | L |
| 17 | H | M | L | VL |
| 18 | H | H | H | VVL |

Table 3. Classes of the Proposed Fuzzy System

| S. No. | Fuzzy Class Description | Abbreviation |
|---|---|---|
| 1 | Very Very Low | VVL |
| 2 | Very Low | VL |
| 3 | Low | L |
| 4 | Medium | M |
| 5 | High | H |
| 6 | Very High | VH |
| 7 | Very Very High | VVH |

CH informs about the status of the nodes to CA. If trust is below L then the accused node is black listed and certificate is revoked and the accuser node is removed from the WL. Else if trust is above L the accused node is removed from the BL list and placed in WL. Once the certificate of the accused node is revoked it cannot participate in the network. Revocation time is calculated every iteration.

The system is executed on Ns-2 simulation tool. The computed revocation is calculated as follows

Revocation Time = (Revoked Time – Detection Time) and the result of revocation time for few iteration is observed.

## 3. RESULTS AND ANALYSIS

In The Cluster-based Certificate Revocation scheme has the following advantages over existing certificate revocation schemes:

a. Distinguish between normal nodes and the malicious nodes.
b. False accusation problem is solved.
c. This system is reliable and efficient.
d. Also more easy efficient to revoke the certificate of malicious nodes.

e. Revocation Time is reduced.
f. More security is achieved.

In the following section the real-time results of our proposed method using NS-2 Simulator. The purpose of our system is to evaluate the performance in terms of the revocation time. Malicious node launches the attacks within the multi-hop transmission range.

a. Revoked Time:-
This is revocation time required for revoking the attacker node detected from the network.
b. Detection Time:-
This is the time required to detect the malicious node in MANET.
c. Revocation Time:-
The revocation time is calculated for the entire malicious node. This an important factor for analyzing and evaluating the performance of the revocation mechanism. It is the difference between the revoked time and detection time.

Revocation Time = (revoked Time – detection Time) (1)

The result shows that, graph of number of iterations of malicious node vs. Time (in Milliseconds).

In this section we discuss the real-time results of our proposed method using JAVA language. The purpose of our system is to evaluate the performance in terms of revocation time. Malicious node launches the attacks within the one-hop transmission range.

a. Detection Time:-
Here, we analyze the detection time required for detection of malicious node. Detection time represents the amount of time needed to detect the malicious node in a network.
b. Revoked Time:-
Here, we also analyze the revoked time required for revoking the malicious node from the network. Revoked time represents the time needed to revoke the detected malicious node from the network.
c. Revocation Time:-
Here, we calculate the revocation time for all the malicious nodes. Revocation time is an important factor for evaluating the performance of the revocation scheme. Revocation time is defined as the time from an attacker node's launching an attack until its certificate is revoked.

Revocation Time = (revoked Time – detection Time)

The result shows that, graph of number of iterations of malicious node vs. time (in Milliseconds). Graph with fuzzy logic and without fuzzy logic drawn.

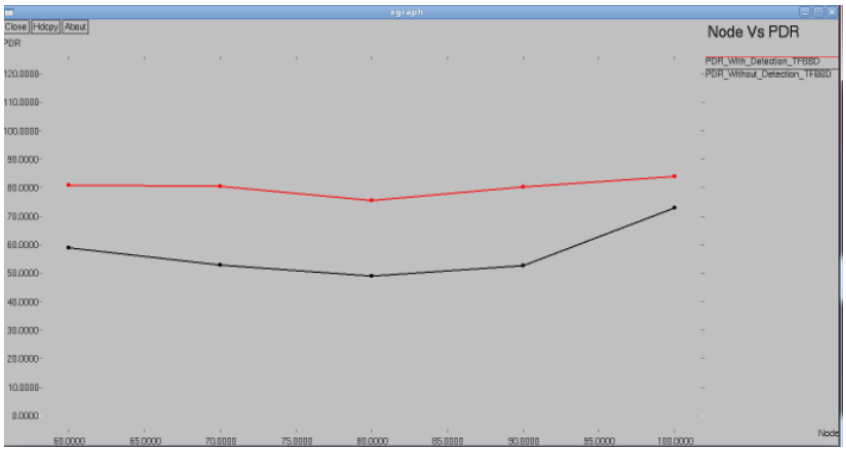


Figure 5. Node vs Packet Drop Ratio

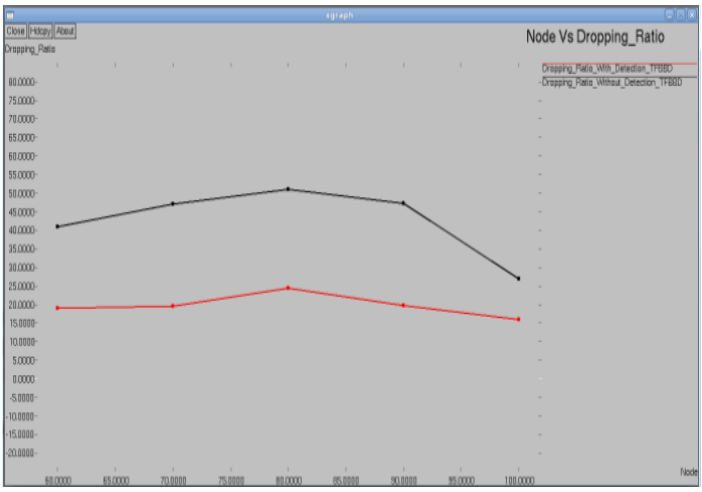


Figure 6. Node vs Dropping Ratio

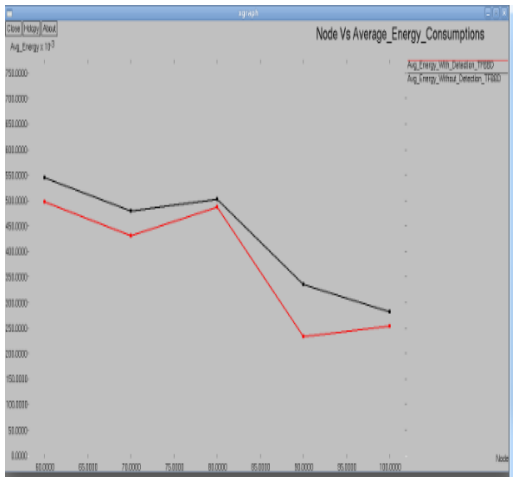


Figure 7. Node vs Average Energy Consumptions

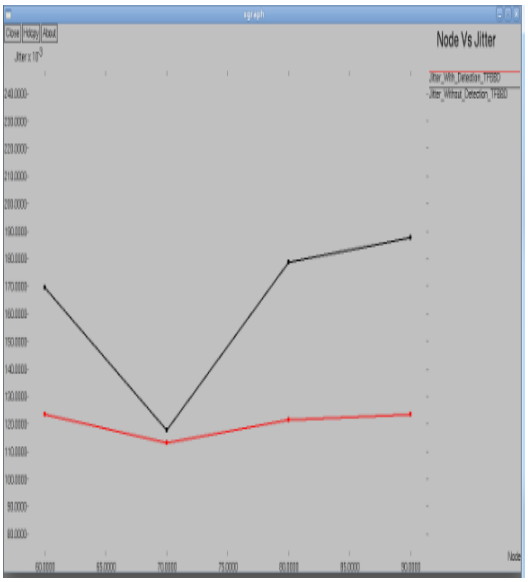


Figure 8. Node vs Jitter

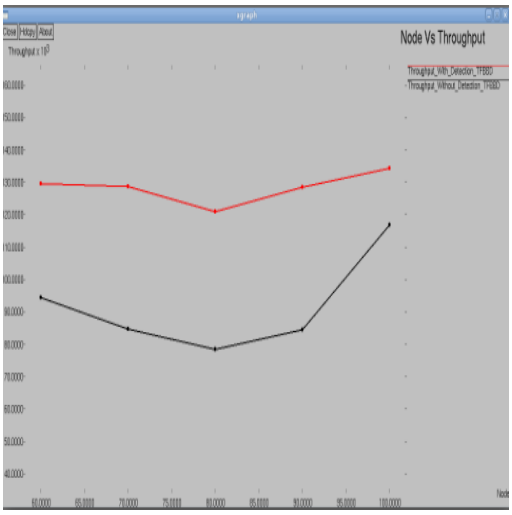


Figure 9. Node vs Throughput

## 4. CONCLUSION

In this paper we discuss the need for Security in MANET, focusing on certificate revocation. Providing security is challenging tasks due to its key features. Different authentication techniques, Digital certificate and components of Public Key Infrastructure are also discussed. The certificate revocation is a challenging task in MANETs due to absence of centralized repositories and trusted authorities. The various techniques of certificate revocation in cluster based mechanism are compared. The working principle, advantages and disadvantages of certificate revocation are compared. And the latest type of Certificate revocation techniques using fuzzy is discussed with reduced overhead.

In near future we will use fuzzy cost which will be evaluated on the basis of the residual energy and the node centrality. The fuzzy cost will be dynamic in nature as it will be evaluated in each round. Thus will provide more better results due to its adaptive nature i.e. will change as the residual energy changes. The main advantage of this suggested protocol is that the optimum numbers of clusters will be formed in every round, which is almost impossible in LEACH and also not guaranteed in EDDEEC.

## REFERENCES

[1] Richhariya, V., & Kaushik, P., "A Survey on Network Attacks in Mobile Ad Hoc Networks", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.4, no. 5, pp. 131-133, 2014.

[2] Muniyal, B., Prakash, K., & Sharma, S., "Wireless public key infrastructure for mobile phones" arXiv preprint arXiv:1212.2563, *International Journal of Network Security & Its Applications (IJNSA)*, vol.4, no.6, 2012.

[3] Forné, J., Muñoz, J. L., Esparza, O., & Hinarejos, F., "Certificate status validation in mobile ad hoc networks", *IEEE Wireless Communications*, vol. 16, no. 1, pp. 55-62, 2009.

[4] BW Yohanes, HK Wardana., "Focused Crawler Optimization Using Genetic Algorithm", *TELKOMNIKA Telecommunication, Computing, Electronics and Control*. 2011; 9 (3): 403.

[5] Jose, J., & Sasi, S. B., "*Certificate revocation in MANET using clustering*", In Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference, 2015, pp. 1-3.

[6] Attokaren, A. G., & Mujeebudheen Khan, A. I., "Survey on Certificate Revocation Scheme for Mobile Ad Hoc Networks", *International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 3410-3415, 2014..

[7] Luo, H., Kong, J., Zerfos, P., Lu, S., & Zhang, L., "URSA: ubiquitous and robust access control for mobile ad hoc networks", *IEEE/ACM Transactions on Networking (ToN)*, vol. 12, no. 6, pp. 1049-1063, 2004.

[8] Liu, W., Nishiyama, H., Ansari, N., Yang, J., & Kato, N., "Cluster-based certificate revocation with vindication capability for mobile ad hoc networks", *IEEE Transactions on parallel and distributed systems*, vol. 24, no. 2, pp. 239-249, 2013.

[9] Khandelwal, V., & Goyal, D., "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 2, no. 4, pp-1555-1559, 2013.

[10] Prakash, G., Vyas, B., & Kethu, V. R., "Secure & Efficient Audit Service Outsourcing for Data Integrity In Clouds", *International Journal of MC Square Scientific Research*, vol. 6, no. 1, pp. 5-60, 2014.

[11] Awadalla, M. H. A. "Heuristic Approach for Scheduling Dependent Real-Time Tasks", *Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 3, pp. 217-230, 2015.

[12] Audah, L., Sun, Z., & Cruickshank, H., "QoS based Admission Control using Multipath Scheduler for IP over Satellite Networks", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 2958-2969, 2017.
[13] Tamizharasi, A., Selvathai, j.j., Kavi priya, A., Maarlin, R., Harinetha, M., "Energy aware heuristic approach for cluster head selection in wireless sensor network", *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 1, pp. 70-75, 2017.