Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Optimized Solutions to Cryptography for Securing MANETs and Analyze Using Reputation System

Rooz Munjal
Research Scholar , CSE Department, JMIT, KUK, India.

Pinki Tanwar
Assitant Professor CSE Department JMIT, KUK, India.

Nitin Goel
Microsoft Patent Research Engineer /Services , CPA Global. Noida , DELHI, India.

Abstract— :- MANET is a self-configuring network of mobile hosts or routers without any pre-deployed infrastructure, centralised policy and control. Initially, ad hoc routing has focused on the problem of providing efficient mechanisms for finding paths in very dynamic networks, without considering security . Because of this, there are a number of attacks that can be used to manipulate the routing in an ad hoc network. Due to above characterstics securing protocols for mobile ad hoc networks presents unique challenges. In this paper we have focused on secure reputed routing in Mobile Ad-hoc Network. In this paper, we have provided a number of contributions of cryptography which is mode of providing three major services: Authentication, Encryption / Decryption and Key Management so very closely related to security research in MANET.

Keywords— Public Key Cryptography, Threshold Cryptography, Identity Based Cryptography, Elliptic Curve Cryptography, Public Key Infrastructure, Reputation System

I. INTRODUCTION

Current research in MANET has focused on routing security, key management, trust management is associated with fundamental method of data protection in the area of information and network security is *cryptography*, authentication, authorization, encryption, and decryption Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation. The application of cryptography include the use of cryptographic techniques to territory security, military communications, financial transactions, and so on. The method of data encryption and decryption are divided into symmetric encryption and asymmetric encryption. Encryption is the process of encoding plaintext into cipher text and decryption is the reverse process. Through the data encryption and decryption, the protection of data, confidentiality and integrity are achieved.

Symmetric Cryptography (SKC):- The encryption key is closely related to the decryption key in that they are identical in between two or more parties that can be used to maintain private communication. If a symmetric cipher is to be used a good choice would be HMAC with MD5 or SHA-1 i.e. HMAC-MD5 or HMAC-SHA1. Note that the MD5 hash function have many attacks against them; however, this does not effect the security of HMAC-MD5.[1]

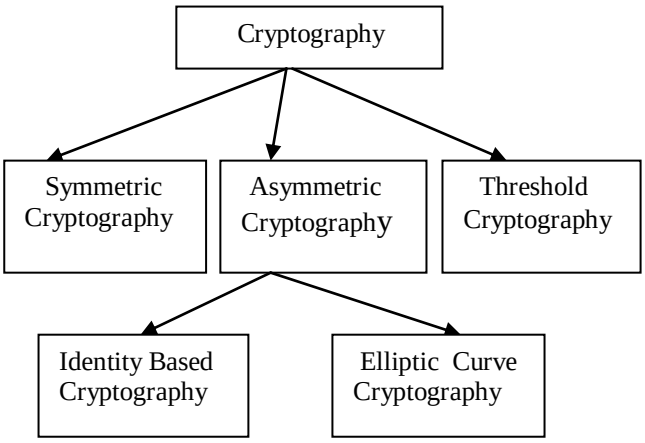

Fig:- Cryptography major components applied in Manet

Asymmetric Cryptography(PKC):- In PKC, each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key where as the public key is distributed to all users taking part in the communication. As encryption key can be made public so it is called as Public Key Cryptography. Some public key

algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. Example: If A wishes to send a message to B, it encrypts the message by using B's public key as the following equation: $E_{KUb}(M) = C$ When B receives the message, B decrypts it by using B's private as the following equation: $E_{KRb}(C) = M$.[1]

Threshold Cryptography:- Threshold Cryptography is used for communication between individual and groups and also used between groups frequently. Threshold cryptography is a technique to execute distributed security functions as demanded in MANETs. In Threshold Cryptography public key is known to all the entities and private key is divided into shares and distributed to entities which are known as Shareholders. In (k,n) threshold cryptography scheme where k is the threshold value and n is the number of secret shareholders. Any at least k out of n secret shareholders are required to collaborate to recover the system's secret while less than k shareholders can never do so. [1]

Outline: The paper is structured as : Section II introduces the MD5 Hash Function and MD5 with Secret Key which is very effective and less power consuming security solution for MANETs. . However, Section III provide a description of Threshold Cryptography used in MANET. In Section IV description of Identity Based Cryptography is provided which is a type of PKC. Section V provides the detail of ECC based energy efficient two party mutual authenticated key agreement protocol suitable for MANETs. Section VI, provided Public Key Infrastructure. Further, Section VII describe different reputation based schemes like CONFIDANT, CORE, OCEAN etc. to discourage malacious behaviour and identify faulty behaviour. In MANETs, reputation systems are often used to deal with routing related problems, like authenticated selfish nodes which do not forward the packets as they should do according to chosen routing protocols.

II. MD5 HASH FUNCTION

The Message Digest algorithm version 5 (MD5), was developed by Ronald L. Rivest (MIT) in 1991. This cryptographic hash function takes as input a message of arbitrary length and produces as output a 128-bit (16 byte) message called *digest* also termed as MD5 hash or checksum which is used to check data integrity. There is a very small possibility of getting two identical hashes of two different files..

MD5 Hash Properties:

Hash length: The most common hash value lengths are either 128 or 160 bits for MD5 and SHA algorithms respectively i.e. hash value is based on algorithm.

Non-discoverability: Two different file even they differ only in single bit translate into two different hash values. But it , can not discover a pair of files that translate to the same hash value.

Repeatability: When a file is hashed using same algorithm many times it will produce same hash value

Irreversibility: Hashing algorithms should be one-way. Message can not be recreated with digest.

MD5 with Secret Key : It is to secure AODV messages is proposed in [3]. It is very effective and less power security solution for MANETs. *Assumption: there exists a central key management system, which provides secret key to all legitimate nodes in advance before they participate in system called a team key or a group key or anything else.

Working of MD5 with secret key:

Every time a node *originates* a RREQ, a RREP or a RERR message, it performs the following operations:-

1. It chooses suitable value of hash function h that is to be used to make message digest, which is 1 for MD5.
2. Sets Hash_Function field by value of chosen h. Hash_Function = h Where, h is the value of hash function means 1 for MD5.
3. Get the value of Secret Key, from central key management system and add it to values of all the fields of message.
4. Calculates Message_Digest by passing the values of all the fields with added secret key to hash function h.

Message_Digest = h (values of all the fields with added secret key) Where, h is a hash function. h(x) is the result of applying the function h to x.

In addition, every time a node *receives* a RREQ, a RREP or a RERR message, it performs the following operations in order to *verify* the valid message :-

Get the value of Secret Key, and add it to values of all the fields of received message. Applies the hash function h to the values of all the fields of received an AODV message with added secure key except Hash_Function and Message_Digest fields, and verifies that the calculated message digest is equal to the value contained in the Message_Digest field of received an AODV message.

Message_Digest = = h (values of all the fields with added secure key except Hash_Function and Message_Digest fields) Where, a = = b reads: to verify that a and b are equal.

Before rebroadcasting a RREQ or forwarding a RREP or a RERR, a node will perform the following:

It once again chooses suitable value of hash function h (may be different of earlier value of h) that is to be used to make message digest. Sets Hash_Function field by value of chosen h. Hash_Function = h Get the value of Secret Key, and add it to values of all the fields of message.

Calculates Message_Digest by passing the values of all the fields to hash function h.

Message_Digest = h (values of all the fields with added secret key)

The concept of MD5 with secret key is shown in fig. below:

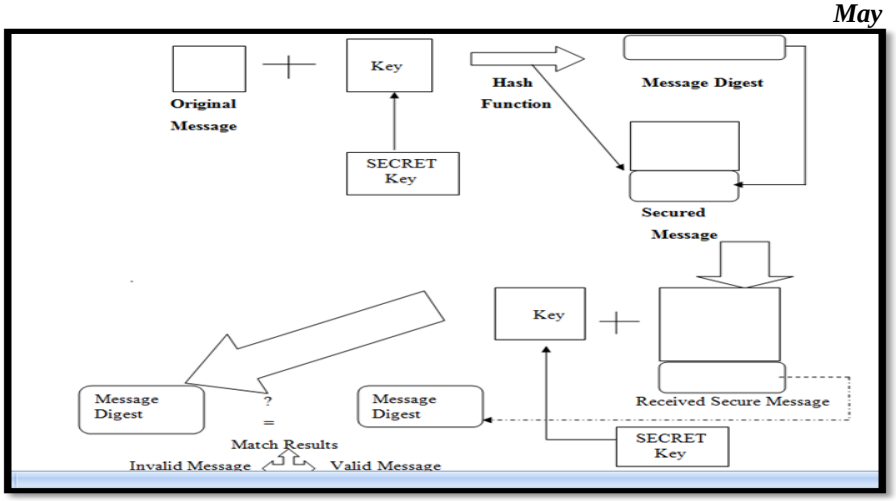

Fig:- Concept of MD5 with Secret Key

III. THRESHOLD CRYPTOGRAPHY

A. ***Secret Sharing:***

allows a group of users to share a secret so that all shareholders can get together and recover the secret. It is unfeasible for less than total no of users to reconstruct the secret. Thus in a (k,n) secret sharing scheme a secret s is shared among n parties satisfying the following requirement

Availability:-greater than or equal to k parties can recover s.

Confidentiality:-less than k parties have no information about s.

B. ***Shamir Secret Sharing*:**

is a (k,n) threshold secret sharing based on polynomial interpolations. To share a secret s among k parties, we do following steps:

i) Let s be secret chosen from z_p , p, prime.

ii) Select a random polynomial:

$f(x)=f_{0+} f_1(x_1)_+$ ------$f_{k-1}(x_{k-1})$ where

f0= s and f1, f2,… fk-1 are chosen randomly from Zp.

iii) For all, $i \in [1,n]$, distribute the share si = (i, f(i)) to the *i*th party.

.Once the secret has been shared, it can now be reconstructed from every subset of k shares by the Lagrange Formula(1) :

$$f(x) = \sum_{i=1}^{k} y\, i \prod_{j=1 j \neq i}^{k} \frac{x - xj}{xi - xj} mod p$$

(1).

The concept of Lagrange's interpolation is finding out missing data with all other data present. Later, Secure Key Sharing (SKS) Scheme was proposed based on Shamir Secret Sharing.

C. ***Proactive Secret Sharing:***

To enhance the security , the servers generate and update a new set of shares for the same Secret based on Shamir secret sharing from the old shares without reconstructing the secret after a given period. This technique come for providing solution when an attacker has the possibility to compromise k-1 server after a given period but he can't compromise k server before this period. This updating of sub shares before the e keeps the system security out of risks of discovering the secret. The update of the sub shares is done as follows:1)generation of the update polynomial *f(x)* then 2) distribution to all network nodes .

3) Updation of shares by all network nodes by adding this polynomial to the old subshare.

D. ***Problem with Threshold Cryptography:***

Threshold Cryptography provides localised security services to MANET. Their operation relies solely on collaboration of threshold no. of directly connected shareholders to service requestor. But what if the sufficient number of shareholders are not present? To provide solution Extended Threshold Cryptography (XTC) was proposed to provide service

IV. IDENTITY BASED CRYPROGRAPHY

It is a type of PKC, and was developed by Adi Shamir in 1984 firstly, which uses the identity of the user as a public key. For example, IKM uses ID-based cryptography .In Identity-based encryption (IBE) public key of any participant is derived from the identity, or any other intrinsic quality, of the participant itself. For instance, the public key of a node can be its IP address. In this way there is no need for a CA, as a public key is bound unambiguously to a specific participant. IBE has 2 advantages:-1) reduced complexity of encryption at sender side and decryption at other side 2) is that a message recipient doesn't need advance preparation or specialized software to read the communication.

A. ***Properties of IBE :***

1) simplifying key revocation 2) key delegation 3) user credentials management. Identity-based encryption requires nonetheless the presence of a Trusted Third Party, called Private Key Generator (PKG), which firstly generates the master key. A node communicates with the PKG via a secure channel, requesting the private key corresponding to its identity its IP address .Afterthat the node can use its private key to decrypt messages sent to it. This scheme shown in Fig:

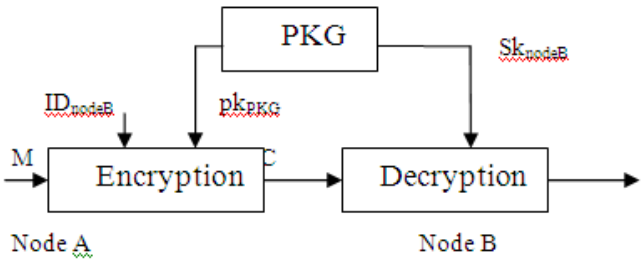

Fig: Identity-based Encryption scheme

B. ***Boneh and Franklin's IBE Scheme:***

Let G be a group with prime order q, e : G × G→Gt be a bilinear map, and g be a generator of G. Let ˆg = e(g, g) ε Gt. Let h1 : {0, 1}* →G and h2 : Gt →{0, 1}* be hash functions. These are all public parameters.

Setup :

PKG picks $s \xleftarrow{R} Zq$. Then g^s is the public key of PKG .

Encryption :

If A wants to send a message m to B, he picks

$r \xleftarrow{R} Zq$ then computes :Encrypt (g, g^s, "B",m)

$= (g^r, m \oplus h2 (e (h1(\text{"B"}), g^s)^r)$

$=(g^r, m \oplus h2(e(h1(\text{"B"}), g)^{rs})$

Making a Private Key :

PKG may compute the private key of An as follows:- MakeKey (s, "B") = $h1(\text{"B"})^s$

Decryption :

Given an encrypted message (u, v) = $(g^r, m \oplus h2(e(h1(\text{"B"}), g)^{rs})$ and a private key w = h1("B")s, B may decrypt as follows. Decrypt (u,v,w)

$= v \oplus h2(e(w, u))$

$= m \oplus h2(e(h1(\text{"B"}),g)^{rs}) \oplus h2(e(h1(\text{"B"})^s, g^r))$

$= m \oplus h2(e(h1(\text{"B"}), g)^{rs}) h2(e(h1(\text{"B"}), g)^{rs})$

$= m$

This scheme was improved by Lynn with the addition of message authentication which guarantees that the integrity of the message is preserved, serving as a digital signature scheme.[6]

V. ELLIPTIC CURVE CRYPTOGRAPHY

is an approach to PKC based on the algebraic structure of elliptic curves over finite fields. The main *advantage* of ECC is its small key size. A 160-bit key in ECC is considered as secured as 1024-bit key in RSA. The *public key* is a point in the curve and the *private key* is a random number. Public key is obtained by multiplying the generator point G in the curve with private key. The Domain Parameters (parameters that must be agreed by both parties) constitutes curve parameters 'a' and 'b', generator point G together with few more constants of ECC. *Security* of ECC comes from difficulty of Elliptic Curve Discrete Logarithm Problem. Let A and B be two points on an elliptic curve such that kA = B, where k is a scalar. Given A and B, it is computationally infeasible to obtain k, when k is large. k is the discrete logarithm of B to the base A. Hence the main operation in ECC is point multiplication. i.e. multiplying scalar k with any point A on the curve to obtain another point B on the curve.ECC is used in the implementation of digital signature generation and verification called Elliptic Curve Digital Signature Algorithm (ECDSA) and key agreement Elliptic Curve Diffie -Hellman (ECDH).[7]

A. ***ECC Based Key Agreement Protocol:***

Based on the elliptic curve DL assumption a new energy efficient two party mutual authenticated key agreement protocol suitable for MANET was proposed. This scheme has used Hybrid Crypto Token (HCT) for computational efficiency. It uses two different cryptographic primitives such as 1) ECC(key pair of MANET node uses ECC)

2)RSA(key pair of TTP is uses RSA) that is why it is named as Hybrid Crypto Token. In HCT, ECC–based public key of a MANET node is being signed by RSA based private key of TTP while in normal digital certificates, key pairs of

both MANET node and TTP are based on same cryptographic algorithms. There are two phases of this Two-Party Authenticated key Agreement Protocol 1) Registration Phase 2) Active Phase

1) Registration Phase:-In this phase Trusted Third Party(TTP) issues a certificate known as HCT to registered MANET nodes. This phase uses RSA primitives, especially for computing the digital signature during generation of HCT. Format of HCT is shown below(Fig).

2) Active Phase:- To conserve the energy of resource constrained MANET nodes, this phase uses ECC-based PKC primitives for generating key pair and symmetric key among MANET nodes and also for generating and verifying signature during authenticated key agreement process.

Field Name	Data Type
Version	Integer
Serial Number	Integer
Signature Algorithm	Hash with RSA Signature
Issuer	String
Valid From	Time
Valid To	Time
Subject name	String
Subject's public Key	Bit String
Thumbprint Algorithm	Hash
Thumbprint	Bit String

Fig:-Format of HCT

Steps of this Two-Party Authenticated key Agreement Protocol:

Step 1: Node A after receiving the node B's beacon verifies its HCT sends an authentication request (AReq(Token$_{A,}$ $Q_{A,}$ RN_A)) message to node B.A selects $r_{A,}$ where $1 <= r_A <= q - 1$ and then computes $QA = r_A \cdot P$. Node A also generate random nonce RN_A

Step2: Node B verifies the A's token using public key of TTP, verification is successful, generates RN_B and computes $SK_{BA} = H((r_B+b)\cdot (Q_A+PubA)||ID_A||ID_B||RN_A||RN_B)$ as a session secret key between A and B.

Step3: Node B computes $HMAC_B = H(SK_{BA}||H((Q_A.x + Q_B.x)||(Q_A.y + Q_B.y)||ID_A||ID_B||RN_A||RN_B))$. It then constructs a message m consists of RN_A, RN_B, Q_B and $HMAC_B$, that is, $m = RN_A||RN_B||Q_B||HMAC_B$ and generates a signature $sig_B(m)$ on m as $sig_B(m) = (r, s)$ using the private long-term key b of B with the help of ECDSA signature generation algorithm. Node B finally sends ARep (m, sigB(m)) as an authentication reply message to node A.

Step4: Node A after receiving ARep verifies signature $sig_B(m)$ using public key of node B with help of ECDSA signature verification algorithm further it checks whether RN_A = ? previously generated RN_A.If both RN_A are equal node A computes session secret key $SK_{AB} = H((r_A+a).(Q_B+Pub_B)||ID_A||ID_B||RN_A||RN_B)$

Step5: Node A compares computed $HMAC_A$ with received $HMAC_B$ for integrity check. If integrity check holds, as an initiator node A ensures successful execution of authenticated key agreement protocol with node B.

Step 6: Node A sends an acknowledgement $(RN_B||HMAC_A)||sig_A(RN_B||HMAC_A)$ to node B.Node B after receiving acknowledgement ,verifies A's signature $sig_A(RN_B||HMAC_A)$ using public key of node A,If this verification holds it checks whether RN_B =? previous RN_B and received $HMAC_A$ =? previous $HMAC_B$. If these hold, it stores SK_{BA} for secure communication with A. [8]

VI. PUBLIC KEY INFRASTRUCTURE

PKI is a trusted framework that must be present to verify the ownership of a public key used in PKC. A PKI is a set of technologies that provides an organization similar levels and forms of trust that exist in the physical world are implemented in the digital world. It includes the hardware, software, policies, people and procedures needed to create, store, distribute, manage and revoke certificates.[1],[10]

A. ***Partially Distributed Certificate Authority(PDCA):***

Based on public key encryption this scheme uses trusted offline CA and (k,n) threshold scheme to protect private key. Offline dealer assigns a valid certificate and public key to the node that join the network. The private key of the node is shared by k serving nodes. The serving nodes are selected randomly in the network. The new node must collect all the n partial key shares to compute the whole private key. This scheme has the drawbacks: i) serving node must maintain public key of all nodes in network, so more memory space. ii) not suitable for larger network. iii) lack of certificate revocation mechanism. iv)no provision of network synchronization when split or join occurs . v) serving nodes may not be in contact at all times.

B. ***Fully Distributed Certificate Authority(FDCA):***Unlike PDCA, the capability of certificate authority is distributed to all the nodes in the network. All nodes in network holds partial share of the private key. Private key is computed by combining any k partial shares. This scheme has the following drawbacks: i) the method doesn't deal with network synchronization ii) threshold parameter k should be larger since attacker may compromise large number of shares between share update iii) complex maintenance protocol.

C. ***Identity based key management scheme(IKM):***The scheme uses set of Private Key Generation (PKG) nodes to generate public key and private key of the node. The public key of the node is generated based on node's identity. A

node must contact at least k PKG nodes to obtain its private key. This scheme reduces communication and computation cost because each node would not have to create its own public key and broadcast it in the network. This scheme doesn't deal with key update

D. ***Self Issued Certificates:*** Unlike IKM, this scheme of no requirement of PKG nodes . Each node create its own private key and certify public key to other nodes, if it has trust on that node. This scheme has the following drawbacks: i) the method doesn't deal with certificate revocation ii) during initial stage, the certificate chain may not be found between all nodes in the network. iii) the system is less trusted without any trusted authority

E. ***Secure Pebble nets:***Secure pebble net is suitable for low performance nodes. Network is partitioned into pebbles, where node with maximum weight is selected as key manager. All nodes in a pebble share a common traffic encryption key for secure communication. It supports group authentication and does not support individual member authentication.

F. ***Cluster Based Composite Key Management Scheme :***This model is given by [9] to solve *problem* of storage in PKI, means each node have to maintain public key of other nodes in network and avoids centralized CA to generate keys, thus enhances security. This is overcome by this cluster based approach. In this approach network is partitioned into clusters (Fig).

Cluster Head: performs two functions: 1) It serves as PKG serving node 2) it plays the role of Key Combiner(private key shares generated by k PKG serving nodes are combined to obtain whole key*).Initial public key* of CH is obtained by applying one-way hash function on its ID and varies with trust value. *New public key* of CH is computed based on old public key and its new trust value. *Initially private key* of CH is assigned by network administrator .Later on, private key shares are computed by PKG nodes.

Mobile Agent: is a program segment that collects information about k trustable nodes (PKG serving nodes) in cluster and nodes whose certificate is revoked.

Hierarchical Clustering Algorithm:

Composite scheme uses hierarchical clustering method, which supports network extendibility. Dominating set based clustering is used for partitioning the network into clusters. The dominator node is selected based on two factors:-

1) Trust Value Evaluation: is based on node's neighbour opinion. When a node sends a packet, it updates packet forwarding status of its neighbour in status table. If packet is forwarded successfully forwarded and unaltered fields in status table are set as 1. Otherwise it is set to 0.After applying AND operation on these fields and then count number of 1's in resultant value. Probability of successful transmission =count/no of forwarded packets >50%, then trust value is incremented.

2) Probability of future contact evaluation: If there exist more than one node with equal trust ability then probability of future contact of node with neighbour is compared by algorithm. Probability is computed based on duration of previous contact and total number of previous contact.

G. ***Zone Based Key Management Scheme:***

This scheme uses ZRP (Zone Routing Protocol) This model is proposed by [12], for each mobile node zone is defined based on some pre-defined number which is distance(in hops) refered to as zone radius (rzone). Symmetric key management is used by mobile node only for intra rzone (zone radius) security while asymmetric key management is used for inter-zone security.

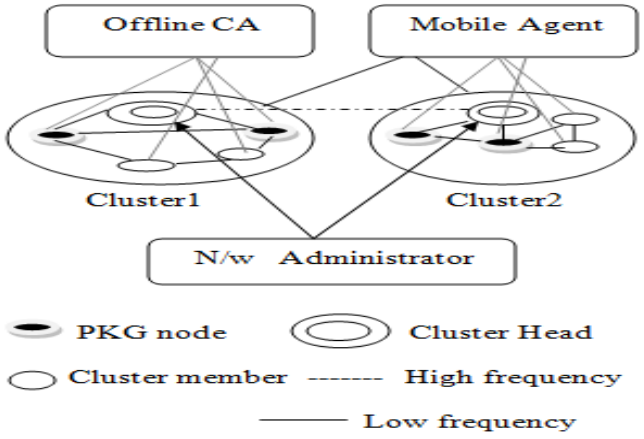

Fig: -Network Structure

VII. REPUTATION SYSTEM

It is a system that takes a feedback from the neighbours of the particular node and provides a mechanism to determine the quality of that particular node based on this feedback. Reputation systems are used in MANETs to address the threats arising from uncooperative nodes and to mitigate selfishness and stimulate cooperation Many areas of electronic transactions, such as eBay and Amazon uses Reputation Systems[13].

A. ***CONFIDANT:***

Buchegger and boudec presented a reputation based protocol called CONFIDANT in 2002 for making misbehavior unattractive. CONFIDANT stands for Cooperation of Nodes : Fairness in Dynamic Ad-hoc Network [14]. Goal is to make it unattractive to deny uncooperation by detecting and isolating uncooperative nodes.

Algorithm:

Let S1,S2,--------SN be N nodes,, where S1 consists of(S1m,S1tm,S1rs ,S1pm) and so on.

Here ,

S1m =monitor of node s1

S1tm= trust manager of node s1 whereS1tm = (AT(type, protocol violations), TT(node, trustlevel) , FL(Friends list))

AT=Alarm Table

TT=Trust Table

FL =Friends List

S1rs=reputation system of node s1

S1pm=path manager of node

Step1:

S1m monitors the neighbouring node and detect misbehaviour by transmission of next node or by behavior of route protocol

Step2:

S1m ⟶ S1tm

ALARM(type , protocol violations)

Incoming ALARM messages comes from Monitor.

Outgoing ALARM messages are generated by the node itself after having experienced, observed, a report of malaci--ous behavior. .

Step3: Source of ALARM (type, protocol violations) is checked for trustworthiness using TT(node, trustlevel) before triggering a reaction.

Step4: After a suspicious event is detected by S1, Event is checked whether event has occurred more often than a predefined threshold that is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions. S1rs updates **rating** of node that caused the event.

Note* For avoiding centralised rating local rating lists and/or black lists are maintained at each node and potentially exchanged with friends.

Step 5:

If **Rating** becomes intolerable, information is given to S1pm.

Step6:

S1pm performs 3 functions:

1)Deletion of paths containing malicious nodes,

2)Action on receiving a request for a route from a malicious node (e.g. ignore, do not send any reply)

3)Action on receiving request for a route containing a malicious node in the source route (e.g. ignore, alter the source).

Advantage:- During the route discovery, node try to avoid is the routes contain node with bad reputation Meanwhile, there no data forwarding service is provided for low reputation nodes as punishment.

Disadvantage:-Sharing only negative information prevents false praise attack, but also have some problems:1)Nodes can not share their good experiences, thus a malicious node can launch a Bad-Mouth attack.

B. ***CORE:***

P. Michiardi et al. proposed a mechanism called CORE (COllaborative REputation mechanism) in 2002[15].Core mainly differentiate between selfish and malacious nodes.

Algorithm:

CORE(WatchDog(WD),ReputationTable(R))

M →Malacious node

X→Any Node

S→ Selfish node

SR[n]= Collection of Subjective Reputations

IR[n]= List of the recent Indirect Reputation values provided by other entities.

FR= value of the reputation evaluated for a predefined function.

RT(ID,SR[n],IR[n],FR[n]) where n = no of nodes

IF X→M

THEN node's subjective reputation value is changed by using WD (watchdog) mechanism.

ELSE IF X→ S OR -ve Reputation Value

All requested by X will be rejected and X works only as service provider not as requester. For long period of time if this node will provide correct services to all other nodes in MANET, node can achieved their reputation value again.

WHILE(X's Reputation Value>>threshold reputation value) **DO**

X will work as service provider as well as service requester.

ELSE

The weight combine formula is used for calculation of functional reputation value.

Advantage :-It resists to attacks due to security mechanism itself: no negative ratings are spread between the nodes, so that no malicious node can decrease another node's reputation. This allows the nodes of the MANET to gradually isolate selfish nodes: when the reputation assigned to a neighbouring node decreases below a pre-defined threshold, service will not be provided by the misbehaving node.

Disadvantage:-It is mainly used for solving the problem of selfish nodes, not efficient for dealing with other malacious problems. It is single layer reputation system which gives equal weight to both first hand and second hand information.

C. ***OCEAN:***

S. Bansal et. al. proposed an Observation-based Cooperation Enforcement in Ad hoc Networks in 2003[16]. This scheme is not allowed to exchange the second hand knowledge about nodes to other nodes in MANET.

Algorithm :

Let S1,S2,--------SN be N nodes,, where S1 consists of (S1nw,S1rr,S1rbr,S1mtr,S1scm) Here, S1nw=Neighbour Watch
S1rr=Route Ranker
S1rbr=Rank Based Routing
S1mtr=Malacious Traffic Rejection
S1scm= Second Chance Mechanism
X→Neighbouring Node of S1
M →Malacious Node
FL[ ]→Faulty List
AL[ ]→Avoid List

Initially Rating of S1,S2,--------SN =0
Let S1 be the node .
IF X→M then
S1nw ⟶ S1rr
Report
S1rr→Decrease rating of X by (-2)
WHILE (Rating of X<<-40) **DO**
X→FL[ ]
S1rbr→adds a AL[ ] to RREQ to avoid routes containing nodes in FL.
S1mtr→rejects the traffic from X.
S1scm →Remove X from FL[ ] after timeout period of inactivity and rating is not increased.
IF X→M **THEN**
X→FL[ ]
END
ELSE
S1nw ⟶ S1rr
Report
S1rr →Increase rating of X by (+1)

Drawbacks of OCEAN: 1) When there is high mobility, OCEAN is very sensitive to change of threshold parameter while second hand protocols like CONFIDANT and CORE are more consistent over varying threshold limits. 2) When the no. of misbehaving nodes is less, its performance falls drastically.

Later, Secure and Objective Reputation-based Incentive (SORI) scheme came in 2004, Afterwards, Locally Aware Reputation System (LARS) came there in 2006. Recently, in 2012 a reputation-based trust management system for detecting and preventing MANET vulnerabilities

REFERENCES

[1] Jianmin Chen and Jie Wu,A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks" Department of Computer Science and EngineeringFlorida Atlantic University
[2] Ajay Jangra, Shalini, Nitin Goel, "Prevention And Reaction Based Secure Routing In MANETS", CSE Department, UIET, Kurukshetra University, Kurukshetra, INDIA, Journal of Global Research in Computer Science, Volume 2, No. 6, June 2011
[3] Syeda Iffat Naqvi, Adeel Akram, "Faculty of Telecom & Information Engineering '' Pseudo-random Key Generation for Secure HMAC-MD5 , 2011 IEEE
[4] Mr. Ravindra K. Gupta, Suketu D nayak"Sec.AODV for MANETs using MD5 with Cryptography" , Int. J. Comp. Tech. Appl., Vol 2 (4), 873-878
[5] Seleviawati Tarmizi, Prakash Veeraraghavan, Somnath Ghosh "Extending the Collaboration Boundary in Localized Threshold Cryptography -Based Schemes for MANETs" Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15-17 December 2009
[6] A. Amuthan, B.Aravind Baradwaj " Secure Routing Scheme in MANETs using Secret Key Sharing " International Journal of Computer ApplicationsVolume 22– No.1, May 2011)
[7] http://www.dkrypt.com/home/ecc
[8] Sharad Kumar Verma , Dr. D.B. Ojha, "An Identity-Based Broadcast Encryption Scheme for Mobile Ad Hoc Networks",International Journal Of Computational Engineering Research Vol. 2 Issue 5.
[9] Kavitha Ammayappan , Atul Negi , V. N. Sastry and Ashok Kumar Das ''An ECC-Based Two-Party Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks "
[10] R. PushpaLakshmi, A. Vincent Antony Kumar, "Cluster Based Composite Key Management in Mobile Ad Hoc Networks", International Journal of Computer Applications, vol. 4- No. 7, 2010.

[11] Renu Dalal,Yudhvir Singh,Manju Khari,"A Review on Key Management Schemes in MANET " International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012

[12] ThairKhdour, Abdullah Aref, "A HYBRID SCHEMA ZONE-BASED KEY MANAGEMENT FOR MANETS", Journal of Theoritical and Applied Information Tecnology, vol. 35 No. 2, 2012

[13] Yhiui Zhang,Li Xu and Xiaoding Wang, " A Cooperative Secure Routing Protocol Based on Reputation System for Ad-Hoc networks", Key Laboratory of Network Security and cryptology /Fujian Normal University,Fuzhou,China,Published in Journal Of Communications,Vol.3 ,No.6,November 2008

[14] Buchegger, S. Le Boudec J.-Y., 2002"Performance analysis of the confident protocol "(cooperation of nodes: fairness in dynamic ad-hoc networks)"in MobiHoc'02, IEEE/ACM symposium on Mobile Ad-hoc Networking and Computing

[15] Michirardi, P., Molva, R. 2002. "Core: A collaborative reputation mechanism to encode node cooperation in mobile ad-hoc networks", in CMS'02 Communication and Multimedia Security Conference

[16] Bansal, S., Baker, M., 2003. "Observation –based Cooperation Enforcement in Ad-hoc Networks",arxiv:cs/0307012v2

