Journal of Computer Science 8 (8): 1397-1406, 2012
ISSN 1549-3636

A Policy Based Scheme for Combined Data Security in Mobile Ad hoc Networks

[1]Kartheesn, L. and [2]S.K. Srivatsa
[1]Department of Computer Science and Engineering,
Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV University),
Kanchipuram, Tamil Nadu, India
[2]St. Joseph College of Engineering, Chennai, Tamil Nadu, India

Abstract: Problem statement: In Mobile Ad hoc Networks (MANET) routing protocols, we require a network-level or link layer security. Since without appropriate security provisions, the MANETs is subjected to attacks like network traffic, replay transmissions, manipulate packet headers and redirect routing messages. In order to address these needs, a policy based network management system that provides the capability to express network requirements is required. **Approach:** In this study, we propose a policy based scheme for combined data security which focuses mainly on three policies: Integrity, authentication and Confidentiality. For providing security not only to data, but also for routing information, we calculate the trust indexes of the nodes and the route is selected according to the trust value which improves integrity. Then in order to provide authentication, we propose a Distributed Certificate Authority (DCA) technique in which multiple DCA is required to construct a certificate. Next we propose an RSA based novel encryption mechanism in order to provide Confidentiality among the nodes. Thus, the desired level of security is provided by the system based on the policy of the user by executing the corresponding security modules. **Results:** By simulation results, we show that this scheme provides a combined data security in MANETs and can be used efficiently. **Conclusion:** Our proposed combined data security policy provides complete protection for the data in MANET communications.

Key words: Mobile Ad hoc Networks (MANET), Distributed Certificate Authority (DCA), Certificate Authority (CA), Policy-Based Network Security (PBNS), Vehicular Ad-Hoc Networks (VANETs)

INTRODUCTION

MANET: The transient infrastructure less multi-hop wireless network in which there is the random movement of the nodes is known as Mobile Ad-Hoc Network (MANET). The wireless transmission range has been extended in MANETs due to its multi-hop packet forwarding. Compatibility in different scenarios can be achieved and there is no infrastructure support which has been deployed in advance (Kushwah and Saxena, 2011). MANETs form an arbitrary topology since it is a self-configuring network of mobile nodes which are connected by wireless links. Movements of the nodes are random and so the wireless topology of the network cannot be predicted and changes rapidly. In emergency situations like natural disasters, military conflicts and emergency medical situations the ad hoc networks are very much suitable due to its minimal configuration, quick deployment and absence of a central governing authority. In the absence of readily available infrastructure networks and for networks of various sizes, the MANETs are applied to configure quickly and dynamically. Even in Vehicular Ad-Hoc Networks (VANETs) and defense sector, MANETs are applied. For flexible civilian applications such as traffic monitoring and emergency assistance services, direct communication between vehicles can be achieved without the need of a cellular infrastructure (Nouak, 2010).

MANET security: The MANET routing protocol is susceptible to many forms of attacks, in the absence of some form of network-level or link layer security. In the wireless network where there is no security provisions the monitoring of network traffic replay transmissions, manipulate packet headers and redirect

Corresponding Author: Kartheesn, L., Department of Computer Science and Enggenering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV University), Kanchipuram, Tamil Nadu, India

routing messages seems to be simple. Maintaining the "physical" security of the transmission media in wired infrastructures and routing protocols is quite harder in practice with MANETs (Garg and Mahapatra, 2009). The route discovery and the data transmission phases of MANET communication needs to be protected in order to provide comprehensive security. Though the correctness of the discovered topology information are guaranteed by the routing protocols, the secure and the uninterrupted delivery of transmitted data is not guaranteed. This is due to the fact the adversaries obey with the route discovery and place themselves on exploiting routes.

This causes random interference with the in-transit data and network operation degradation. The spiteful disruptions of data transmission cannot be rectified using the upper layer mechanisms such as reliable transport protocols or reliable data link and acknowledgement routing which are presently assumed by the MANET routing protocols. While there is no communication between the nodes, the data flow is considered to be undisputed and so the communication nodes are easily betrayed for long periods of time. By protecting and verifying all control and data traffic cryptographic, the security attacks can be contradicted. Appropriate trust relationships need to be established with each and every peer that are transiently associated inclusive of the nodes that forwards their data. Due to denial of service attacks, the cryptographic protection is not feasible and this simple discards the data packets (Mamatha and Sharma, 2010).

Threats in MANET: The security in MANETs is subjected to numerous threats as described below:

- The communication channel is highly insecure in MANETs due to its nature of wireless communication and this also leads to Eavesdropping and masquerading
- Unreceptive control of mobile nodes leads a problem in the node security. Cellular nodes theft has been increased and so the MANET nodes are not secure. The node is negotiated and acts as an unreceptive node
- Node tampering is also caused due to theft and this may interrupt network operations or discharge critical information
- The attacker in the denial of service attack can create additional transmissions or expensive computations which are due to the limited powers in the mobile nodes
- Traditional solutions which are based upon the certification authority and on-line servers cannot be used due to infrastructure-less networks
- The routing protocols become too complex due to the absence of fixed topology. It is quite difficult for securing such type of protocol when unreceptive nodes are present.

Some of the MANET security threats are.
Active attacks:

- Denial of Service (DoS)
- Jamming
- Masquerade
- Fabrication
- Modification

Passive attacks:

- Release of message content
- Traffic Analysis

Apart from the usual threats, achieving security within the ad hoc networking is challenging due to following reasons: Wireless Environment, Absence of Central authority, Selfish Nodes, Dynamic Topology, Limited Computational Capability.

Data security: Data security mainly focuses on the following criteria.

Confidentiality: The information about the data and the routing should be received only by the nodes which are permitted to access the information.

Integrity: Since the information can be corrupted by malicious attacks and benign failure like radio propagation impairment, the data should not be revised during transit.

Authentication: The sender should be correctly identified by the receiver and no other sender can be disguised as the sender.

Availability: Operation of the network is not affected by the DoS attack. Physical jamming, disconnection and malfunction of key management service and routing protocol attacks can be commenced at any layer of the network.

Non-repudiation: In order to detect and isolate the compromised nodes the sender is restricted from false denial of a message.

A policy based network management system which provides the ability to express network requirements is used in order to address the above needs. The network

administrator is given an ability to specify high-level policies in this approach which are as follows.

The aim of long-term, network-wide configuration needs to be specified, e.g., encryption for all private communications is required.

To trigger the correction of network problems based on policies automatically, an automatic feedback loop is required. This triggers the information reported by monitoring agents.

The policy enforcer automatically enforces the policies once after they were described. To configure, control and reconfigure their network in response to network conditions these capabilities provide military personnel with powerful tools (Singh *et al*., 2010). The following section describes some of the existing policy based approaches.

Problem identification and proposed a solution: In our proposed work, we will design security policy with the following functions.

For confidentiality: Depending on different application requirements, the payload part may be optionally encrypted with the shared key between the source and the destination.

For authentication: We use a reactive certificate distribution mechanism using multiple Certificate Authority (CA) nodes. Nodes trusting and being trusted by more than one CA should apply for a certificate and private-key-shares from each CA. A node without Certificate or needing to renew his certificate must ask to other nodes in the MANET for a certificate issuing.

For integrity and drop: We use a Trust based packet forwarding scheme for mitigating the data drop attacks. It uses trust values to favor packet forwarding by maintaining incentives and penalties for each node. Each intermediate node marks the packets by adding its hash value and forwards the packet towards the destination node. The destination node checks the incentives and penalties and verifies the hash value for nodes with low incentive and high penalty.

Depending on the nature of data and user requirements, policies with the following choices are held by any user:

- Any one of CONF, AUTH and INTEG
- All of CONF, AUTH and INTEG
- CONF and AUTH
- AUTH and INTEG
- CONF and INTEG

where, CONF-confidentiality, AUTH-authentication, INTEG-integrity. The desired level of security is provided by the system based on the policy of the sender and receiver. Hence our proposed security policy can provide complete protection for the data in MANET communications.

Related work: Suresh and Duraiswamy (2011) have proposed a node reputation scheme for reactive routing protocol in MANET security. Their scheme also offers an accep trade-off between delay and uncertainty. Their mobility based node reputation scheme identifies and monitor the node's trustworthiness in sharing the information within the ad hoc network. The proposed reactive schemes offer node authentication and reputation. They also handled mobile nodes information uncertainty with the mobility characteristics and its reputation is evaluated to trust or discard the node's communication.

Alicherry *et al*. (2009) have introduced a novel distributed security policy enforcement architecture that is designed specifically for MANETs. Their approach harnesses and extends the concept of network capabilities and is especially suited for mobile and heterogeneous communication environments. Their model imposes communication restrictions between MANET nodes by enforcing hop-by-hop policies in a distributed manner.

Singh *et al.* (2010) have made the traditional approach to security inadequate. With this view in mind decentralized group key management is taken into consideration.. The network considered is not very highly volatile. So we have to investigate the group key management for highly volatile network.

Singh *et al*. (2010) have proposed a novel structure of the node and each entity holds a secret share SSI of each node in a cluster is controlled by its cluster head, the policy enforcer decides for the working of intelligent agent, which is assigned to do the management, which allows two or more parties to derive shared key as a function of information associated with the protocol and so no party can predetermine the resulting value. The group membership certificate is used for group authentication and by the use threshold key scheme secret data are transferred.

Li *et al.* (2009) have proposed and developed a policy-based malicious peer detection mechanism, in which context information, such as communication channel status, buffer status and transmission power level, is collected and then used to determine whether the misbehavior is likely a result of malicious activity or not.

Cheng *et al*. (2010) have presented a Policy-Based Network Security (PBNS) management approach for

tactical MANETs. This approach leverages the DRAMA policy based network management system and the Smart Firewall system to meet the above requirement. It allows administrators to specify low-level network access control policies for each INFOCON level using high-level policies.

Jaisankar *et al*. (2009) have proposed a novel agent based framework to monitor, detect and isolate misbehaving nodes in the MANET. The proposed framework protects both routing and data forwarding operations, which aiming at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead. In their work local neighboring nodes collaboratively monitor each other. A novel honesty rate strategy is introduced in each node to determine the well-behaving nodes.

MATERIALS AND METHODS

Trust based packet forwarding scheme:
Trust index calculation:

Let:

Z = $\{N_1, N_2, \ldots Nn\}$ be the network of nodes.
T_i = The trust index of node N_i,
T_{inc} = The value of trust increment,
T_{dec} = The value of trust decrement,
T_{th} = The trust threshold value.
N_k = The node which forwards a data packet P_k
p = A positive constant for trust increment and decrement.

Algorithm 1:

1. Initially, each node maintains a lookup table, which includes sequence numbers, source and destination IP addresses and port numbers and the address of the next hop.
2. Node N_i receives the data packet P_k.
3. If P_k is a retransmitted packet, then
   3.1 Nodes i decrements trust index of N_k by
   $T_{dec} = T_{dec}\tilde{}2*p$
   3.2 Compare T_{i-1} with $T_{th.}$
   3.3 If $T_0 < T_{i-1} < T_{th}$,
   Packet is dropped.
   Else
   The packet is forwarded to node $N_{i+1.}$
   N_i updates the lookup table with current trust values.
   End if
   Else
   If P_k is an acknowledgement packet, then
   If N_k originally forwarded P_k, then
   N_i increment trust index of N_k by
   $T_{inc} = T_{inc} + p$
   End if
   End if

Route selection for integrity: Let:

- Ti be the Trust index on the individual neighbor
- Ta be the average of the trust index of all the neighbors that forwarded/generated RREP
- Oi be the number of Hops in the route established by the individual node in its RREP, Oa be the average of all Oi's obtained from individual neighbors which forwarded the *RREP*
- CRS_A and CRS_B be the Cost of route selection of the node A and node B respectively
- Tr (A) and Tr (B) be the trust index of the nodes A and B respectively which represents the trust index of the individual neighbor for a Route
- N_{hi}^{A} and N_{hi}^{B} are the trust index of highest immediate downstream neighbors of the nodes A and B respectively

Algorithm 2: The trust index of all the nodes is calculated and then the source node calculates the Cost of route selection (CRS) for all its available routes to the destination using the formula:

$$CRS = (Ti / Ta) * (Tr) * (Oa/ Oi)$$

2. If $CRS_A = CRS_B$, then
   If Tr (A) > Tr(B), then
   Select route A.
   2.2 Else if Tr(A) = Tr(B), then
   2.3.1 If $N_{hi}^{A} > N_{hi}^{B}$
   Select N_{hi}^{A}
   2.3.2 Else if $N_{hi}^{A} = N_{hi}^{B}$
   Select the shortest route.
   End if
   End if

Distribution of certificate authority among cluster heads:

- Initially each node calculates its trust index using the above method. Each node gets the trust value of all its neighboring nodes
- The node with the highest trust value is taken as a cluster head in that particular cluster
- DCA algorithm is proposed, where the DCA private keys are distributed amongst CHs and become the shareholder DCA nodes
- The CH can satisfy this role since it holds the positions of responsibility and has direct communication with one another

- The distribution of the DCA private key is processed and it is maintained among the cluster heads. A shares of the DCA private key need to be issued when a new CH joins the backbone
- Initially, the node contacts their CH when a node looks for a DCA service and it then takes up the request with other CHs

We will define our DCA by specifying the following operations:

- System setup or bootstrapping
- Applying a DCA private key
- Joining a new CH
- Evicting an existing CH
- Updating CH shares

Here, a and b are large primes such that b divides a-1 and s is a generator of the subgroup Sb of Za of order b. The values a, b and s are public system parameters. In addition, let h be a hash function whose range is {1 . . . b-1}.

Bootstrapping: Let, C be the initial set of CHs at a system setup time, |C| = l and m be the required threshold of co-operation between CHs.

All the CHs participating in the shared key construction is required for the establishment of a (m, l) threshold sharing of a private key. In the construction of the NTDR backbone, this CHs participation is just a part. The following Distributed Key Generation (DKG) algorithm is used.

Each CHi chooses v_i in Za and calculates $e_i = sv_i$ mod a.

CHi creates a (m,l) threshold sharing of the secret value v_i by generating a polynomial.

Function $f_i(z)=\sum_{t=0}^{r-1} u_i$, tx^t of degree at most r-1 with f_i (0) = v_i mod u.

In order to distribute the subshare fi(j) to CHj, Chi uses a secure unicast channel (i.e) (n-1) secure unicast channels is required by the Chi.

CHi broadcasts the values ei,t = svi mod a. The consistency of the subshares is verified by these values and are sent by CHi. Let Et = ∏i€C ei,t , where t €{0 . . . r-1}.

Each CHj verifies that the subshare fi(j) received from CHi is valid by checking that:

$$s^{fi(j)} = \prod_{t=0}^{r-1} (e_{jt})^{j^t}$$

Only if this condition is satisfied, we consider the value received from Chi is accurate. Else the other CHs receives a broadcast message from CHj, a warning that an inconsistent subshare has been received from Chi. Then Chi is excluded if at least k warnings related to Chi is received.

Take C1 be the set of consistent CHs at the end of the last stage. Each CHj in C1 computes dj = $\sum_{i€C1}$ fi (j) Each of the consistent CHj holds a share dj of the DCA private key PrK = $\sum_{j€C1}$fj (0), at the end of this protocol. PuK = $\prod_{j€C1} e_j$ is the DCA public key and it is computed from broadcasts exchanges.

Applying a DCA private key: Delivering a DCA security service by a DCA private key is exhibited here. The DCA private key is not known by any CH and its construction shouldn't be done during any application. A node where a DCA digitally signs a request REQ is considered. The request is forwarded to the backbone. The share of SK can be used by any other CH receiving a request, in order to sign the request and to produce a signature share, prior to sending it back to the requesting node. The DCA signature can be constructed on REQ when the node has verified k signature shares. A threshold signature scheme is used for the accomplishment of this process. A variant of the digital signature standard is presented here.

Let:

d €Z_b = private key
e = s^d mod a
(a, b, s, e) = Public Key

To sign a message ϕ, first compute η=h (ϕ), generate a random number w €Z_b and then compute:

ρ = (s^w mod a) mod b
ψ = ρl + wη mod b

We denote the signature on message ϕ given by (ρ, ψ), as:

ρ = ($s^{\psi/\eta}$ $e^{-\rho/\eta}$ mod a) (mod b)

The following (m, l) threshold signature scheme based upon the prior variance of DSS, is assumed here Let C2 $\underline{C}$ C1 (where |C1| ≥ m) is the set of CHs available to assist in signing request REQ.

Initially a random value e is distributed. In C2 the CHs show an example of the DKG algorithm. Adequate consistent CHs are assumed and the result is a subset C3 of consistent CHs. This shows that each Chi € C3 has a wi share of a random value w. The following public values exist:

$M = S^w \bmod a$
$P = \mu \bmod b$
$H_t = \prod_{i€C3} S^{hi,t}$

where, t € {0,…., r-1} and $h_{i,t}$ are CHi's polynomial coefficients. During this process, the w is not exposed to any CH.

Compute $\psi_i = \rho\, d_i + \varepsilon\, (REQ)\, w_i \bmod b$ in each Chi of C3 and taking that the |C3| must be greater than m, send it to the requesting node.

The consistency of the value is verified using the following equation after receiving each δl:

$$s^{\Psi t} = (e)\prod^{m-1}(Ej)^{tj})\rho_{j=1}(\mu\prod^{m-1}(Hj)^{tj})^{\varepsilon(REQ)}_{j=1}$$

4. Using Lagrange formula to {ψi}, ψ can be computed by the requesting node:

$$\psi = \sum\prod^{m}_{q\neq j_{j=1}} i_q / (i_q - i_j) \text{ for any } CH_{i1},.....CH_{jk} \notin C3$$

Share updating:

Update Initialization: In order to ensure that only one initialization node group is present within the whole system, update initialization is done. This corresponds to finding one CA node forming a group with t CA server nodes. Following measures are taken in order to update initialization:

- An initialization message is broadcasted by the selected CH to all other CH in the neighboring clusters. The message carries an update request and the ID of the sending CH
- The probability of multiple initializations is reduced by adopting a backoff scheme. After the random backoff period is over the CH broadcasts the message
- We determine the length of the backoff period as:
- In the range [0, CwS], the CH chooses an integer Wi. Contention window size is denoted by CwSi. Prior to broadcasting of the initialization message in the backoff state, the node waits for (wSi × Ts) seconds, where Ts = Time slot size which is common to all CHs
- CHi monitors the received messages during the backoff period. The backoff state is terminated on receiving any initialization messages from other CHs and the node starts preparing for the share updating.
- If the node doesn't receive initialization messages, at the end of the backoff period, the node sends an initialization message which floods among all CHs. The involved overhead is inhibited even for large MANETs, due to that the flooding is restricted only in CHs

The trust value keeps changing and so the cluster head is also changed. By this we can share the updating of the message to all other nodes.

Determination of ts and CwS: The CH with the largest propagation delay within the MANET is selected as the appropriate Ts. The collision of the initialization messages can be avoided by choosing two CHs whose wSi differ by 1.

If CwSi is small, the chance of a collision increases, but it leads to a prolonged backup time when the CwSi increases. The number of CH nodes is the suitable choice for CwSi.

It is enviable to prioritize the CH nodes which have enough CA in its cluster or in neighboring clusters, when t CA server nodes are participating in the derivation of new shares.

Generally, we can divide the contention window (CwS) size into three categories.

CH nodes having more than t CA nodes in the cluster-Wa

CH nodes having less than t CA nodes in the cluster, but more than *t* CA nodes plus the CA nodes in the direct neighboring cluster-Wb

The remaining CH nodes assigned largest CwS value - Wc

The probability of selecting a CH increases when the CHs has more CA nodes in its neighborhood.

Multiple initializations can still be avoided using the collision resolution method:

- An acknowledgement is sent to the receiver when a CH receives the initialization message.
- The ID of the messages is compared by CH, when a new initialization message is received.
- The node ID is checked for the newer message and if it's a smaller one, then the node sends ACK to the new sender NACK is sent to previous sender.
- After all ACKs are collected from the CH node the winner is determined.

Update procedure: At the end of update initialization, the winning CH node is represented as Q. New shares are derived as Q finds t CA nodes.

Update propagation: At least t servers has updated their shares at the end of the update procedure. The remaining CA nodes in the network are updated by the t updated servers. The share updated is propagated to all the CA in this phase. The CH is informed about the update completion when CA finishes the share update process. The data regarding the completion of the information from its local cluster is collected by the CHs and the neighboring CHs that has no updated

information is informed about it. For the update information the informed CHs sends a request to the CA nodes. Based upon the locating method described above, the CAs will then contact the CHs for locating t CAs with new shares.

Providing data confidentiality using encryption: The security scheme consists of RSA key exchange mechanism and a novel encryption mechanism to provide security:

- Each node in the network has its own symmetric key Nkey
- To perform encryption and decryption, each node must know other node's Nkey
- At source, Nkey is encrypted with PUr and transmitted to the destination and destination, decrypts Nkey with PRr, where PUr and PRr are the public and private keys of the receiver, respectively

Encryption: The data M is encrypted using the data specific key and the data specific key is encrypted with Nkey. Then, the sender appends the destination nodes ID and transmits this message to its authenticated neighbors.

Initially, source node A creates a Data Key Dkey.

The data is encrypted with Dkey, $[E_{Dkey}(M)]$.

Then the DKey is encrypted with A's Nkey $[E_{NkeyA}(Dkey)]$.

Then, the Destination node's ID is appended to the Cipher text:

$[E_{NkeyA}(Dkey), [E_{Dkey}(M), DestID]$

Decryption: The plain text message is obtained only if the ID of the node matches and it is considered as the intended recipient. The decryption is performed with Nkey of the sender. In order to obtain the original message the decryption is done with the Dkey. The node again re-encrypts the message if it is not an intended recipient. Re-encryption is done with the neighborhood key and it is transmitted to the authenticated neighbor nodes. Once the destination is determined and the original message is decrypted at the destination, the process is stopped.

In the ad hoc network where more attacks can occur, the encryption of the message by Nkey and Dkey provides more security while data forwarding:

Algorithm 3:

1. Source node A creates Dkey
2. Data is encrypted with Dkey, $[E_{Dkey}(M)]$
3. Dkey is encrypted with A's Nkey $[E_{NkeyA}(Dkey)]$
4. DestID is attached with cipher text

$[E_{NkeyA}(Dkey), [E_{Dkey}(M), DestID]$

5. If DestID matches with receiving node,
   5.1 Decryption is performed.
   5.2 Original message is decrypted
   Else
   5.3 Re-encrypts the message
6. Repeat step 5 until the destination node is found.

Policy based scheme for integrity, authentication and confidentiality: Depending upon the nature of data and user requirements, user policies (P) can be specified which can take the following values:

- I-Only Integrity
- Only Authentication
- C-Only Confidentiality.
- IA-Both Integrity and Authentication.
- IC-Both Integrity and Confidentiality.
- AC-Both Authentication and Confidentiality.
- IAC-Integrity, Authentication and Confidentiality

Based on the policy of the user, the corresponding security module(s) can be executed, as per the following algorithm.

Algorithm 4:

1. If Policy = "I", then
   1.1 Calculate the trust index of all the nodes according to algorithm 1 in section 3.1.1
   1.2 Select appropriate routes using the algorithm 2 in section 3.1.2.
2. Else if Policy = "A", then
   2.1 DCA private keys are applied to deliver security service according to section 3.2.1
   2.2 Share updating is done among the cluster heads according to section 3.2.2.
3. Else if Policy = "C," then
   3.1 Encryption and Decryption are done according to the algorithm 3 in section 3.3
4. Else if Policy = "I" and Policy = "A", then
   4.1 Calculate the trust index of all the nodes according to algorithm 1 in section 3.1.1.
   4.2 Select appropriate routes using the algorithm 2 in section 3.1.2.
   4.3 DCA private keys are applied to deliver security service according to section 3.2.1
   4.4 Share updating is done among the cluster heads according to section 3.2.2.
5. Else if Policy = "I" and Policy ="C", then
   5.1 Calculate the trust index of all the nodes according to algorithm 1 in section 3.1.1
   5.2 Select appropriate route using the algorithm 2 in section 3.1.2.

5.3 Encryption and Decryption are done according to the algorithm 3 in section 3.3.

6. Else if Policy =”A” and Policy =”C”, then

6.1 DCA private keys are applied to deliver security service according to section 3.2.1.

6.2 Share updating is done among the cluster heads according to section 3.2.2.

6.3 Encryption and Decryption are done according to the algorithm 3 in section 3.3

7. Else if Policy = “I” and Policy =”A” and Policy =”C”, then

7.1 Calculate the trust index of all the nodes according to algorithm 1 in section 3.1.1

7.2 Select appropriate routes using the algorithm 2 in section 3.1.2.

7.3 DCA private keys are applied to deliver security service according to section 3.2.1.

7.4 Share updating is done among the cluster heads according to section 3.2.2.

7.5 Encryption and Decryption are done according to the algorithm 3 in section 3.3

End if

RESULTS AND DISCUSSION

Simulation results:

Simulation model and parameters: We use NS2 to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 100 mobile nodes move in a 1500×500 m region for 50 sec simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 m. In our simulation, the number of attackers varies from 2-10. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in Table 1.

Performance metrics: We evaluate mainly the performance according to the following metrics.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Drop: It is the number of packets is dropped during the transmission.

Table 1: Simulation Parameters

No. of nodes	50
Area size	1500×500
Mac	802.11
Radio range	250 m
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Mobility model	Random way point
Attack type	Blackhole
No. of attackers	2,4,6,8 and 10
Pause time	5

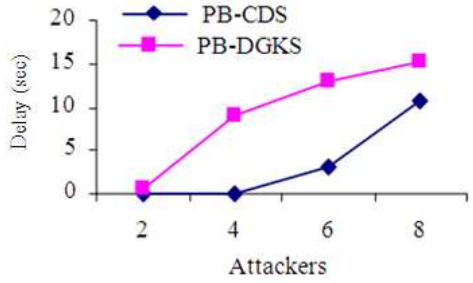

Fig. 1: Attackers Vs delay

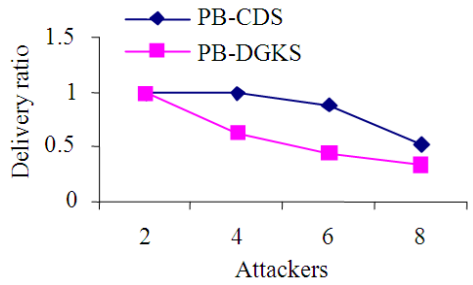

Fig. 2: Attackers Vs delivery ratio

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of receiving data packets.

The simulation results are presented in the next section. We compare our PB-CDS protocol with the PB-DGKS (Singh *et al*. 2010) protocol in presence of malicious node environment.

Based on attackers: In our experiment, we vary the no. of misbehaving nodes as 2,4,6,8 and 10.

Figure 1 shows the results of average end-to-end delay for the misbehaving nodes 2, 4…. 10. From the results, we can see that PB-CDS scheme has slightly lower delay than the PB-DGKS scheme because of authentication routines

Figure 2 shows the results of the average packet delivery ratio for the misbehaving nodes 2, 4…. 10 scenarios. Clearly our PB-CDS scheme achieves more delivery ratio than the PB-DGKS scheme.

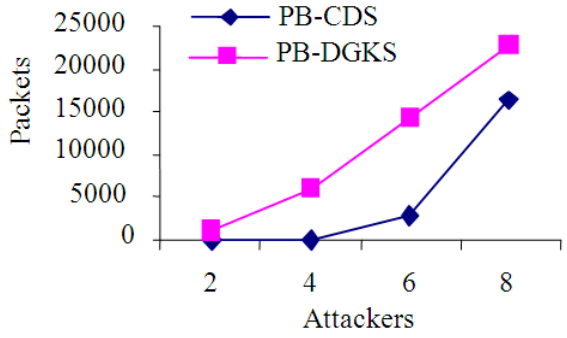

Fig. 3: Attackers Vs drop

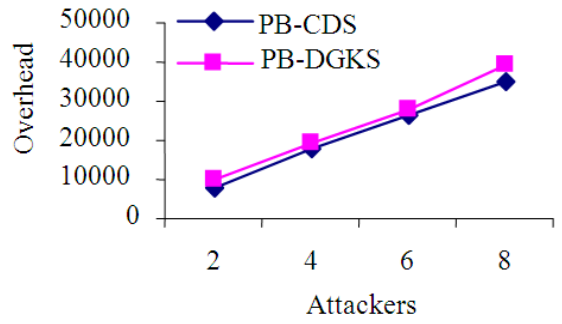

Fig.4: Attackers Vs overhead

Figure 3 shows the results of Packet drop for the misbehaving nodes 2, 4…. 10. From the results, we can see that PB-CDS scheme has less drop than the PB-DGKS scheme.

Figure 4 shows the results of routing overhead for the misbehaving nodes 2, 4…. 10. From the results, we can see that PB-CDS scheme has less routing overhead than the PB-DGKS scheme.

CONCLUSION

In this study we propose a policy based scheme for Combined Data Security which focuses mainly on Integrity, authentication and confidentiality. For providing security not only to data, but also for routing information, we calculate the trust indexes of the nodes and the route is selected according to the trust value. The node with the highest trust value is taken as the source node and the source node calculates the cost of the route selection for all its available routes to the destination. Then in order to provide an Authentication, we propose a Distributed Certificate Authority (DCA) algorithm. Here a DCA private key is distributed among the cluster heads using the threshold signature scheme. Next we propose an RSA key exchange mechanism and a novel encryption mechanism in order to provide Confidentiality among the nodes. In this we use two different symmetric keys to encrypt the message which improves the security while forwarding the data in the ad hoc network. Finally, the user policies can be provided with different probabilities depending upon the nature of the data and the user requirements. From our simulation results we show that this scheme provides a combined data security in MANETs and can be used efficiently.

REFERENCES

Alicherry, M., A.D. Keromytis and A. Stavrou, 2009. Deny-by-default distributed security policy enforcement in mobile ad hoc networks. Secu. Privacy Commun. Networks, 19: 41-50. DOI: 10.1007/978-3-642-05284-2_3

Cheng, Y.H., A. Ghosh, R. Chadha, M.L. Gary and M. Wolberg, 2010. Managing network security policies in tactical MANETs Using DRAMA. Proceedings of the Military Communications Conference, Oct. 31-Nov. 3, IEEE Xplore Press, USA., pp: 960-964. DOI: 10.1109/MILCOM.2010.5679579

Garg, N. and R.P. Mahapatra, 2009. MANET security issues. J. Comp. Sci. Netw. Secu., 9: 241-246.

Jaisankar, N., R. Saravan and K.D. Swamy, 2009. An agent based security framework for protecting routing layer operations in MANET. Proceedings of the 1st International Conference on Networks and Communications, Dec. 27-29, IEEE Xplore Press, India, pp: 381-385. DOI: 10.1109/NetCoM.2009.64

Kushwah, R.S. and A.S. Saxena, 2011. Reactive multihop routing with MCDs in MANETs. Indian J. Comput. Sci. Eng., 2: 885-891.

Li, W., A. Joshi and T. Finin, 2009. Policy-based malicious peer detection in ad hoc networks. Proceedings of the International Conference on Computational Science and Engineering, Aug. 29-31, IEEE Xplore Press, Vancouver, BC., pp: 76-82. DOI: 10.1109/CSE.2009.289

Mamatha, G.S. and S.C. Sharma, 2010. A robust approach to detect and prevent network layer attacks in MANETS. Int. J. Comput. Sci. Secu., 4: 275-284.

Nouak, A., 2010. MANET security. Proceedings of the 6th International conference on intelligent information hiding and multimedia signal processing, Oct. 15-17, Darmstadt, Germany.

Singh, S., N. Rajpal, A.K. Sharma and R. Pahwa, 2010. Policy based Decentralized group key security for mobile ad-hoc networks. IJCSI Int. J. Comput. Sci. Iss., 7: 44-49.

Suresh, A. and K. Duraiswamy, 2011. Mobile ad hoc network security for reactive routing protocol with node reputation scheme. J. Comput. Sci., 9: 242-249. DOI: 10.3844/jcssp.2011.242.249