IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 2, Issue 3 (July-Aug. 2012), PP 40-48
www.iosrjournals.org

Trust Based Packet Forwarding Scheme for Data Security in Mobile Ad Hoc Networks

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

Abstract: *In Mobile Ad hoc Networks (MANET) Threats is a major concern and most routing protocols are based on Authentication, Security Association, key distribution and so on. we require a network-level or link layer security. Since without appropriate security provisions, the Mobile adhoc Networks are subjected to attacks like network traffic, replay transmissions, manipulate packet headers and redirect routing messages. In order to overcome these problems Trust based Packet Forwarding Scheme is suggested for mobile ad hoc Network System that provides the capability to express network requirements. In this paper, we propose a Trust Based scheme for Combined Data Security which focuses mainly on Integrity and Authentication. 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 Distributed certificate authority are required to construct a certificate. Thus, the desired level of security is provided by the system based on the policy of the user by executing the corresponding security modules. Hence our proposed Trust based Packet Forwarding Scheme for data Security provide complete protection for the data in Mobile Ad hoc Network communications.*

Keywords: *Trust Index, Trust Value , Data Security, Mobile Ad hoc Networks, Integrity Certificate Authority, Cluster Heads.*

I. Introduction

1.1 Manet

A mobile ad hoc Network (MANET) is an infrastructure-less network where each node act as router for establishing end-to-end connection and a host for the source or destination. The transient infrastructure less multi-hop wireless network in which there is random movement of the nodes is known as mobile ad-hoc network(MANET).Itisvulnerabletovarious type of attacks that include Jamming Attack [1] External Vulnerabilities like eavesdropping and dynamic network and internal constraints like limited computational and storage capabilities pose challenges in implementing a secure ad hoc Network. Hence basic security requirement of MANET are authentication, integrity, confidentiality, authorization and trust management [2],[3],[4]. 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. [5] 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 [6]. 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. [7]. Each node that participate in the Network provides a service such as routing information, Authentication etc. to form a network with other nodes spread over an area.

1.2 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 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. [8]. 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 is 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 exploited 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 undisrupted and so the communication nodes are easily betrayed for long periods of time. By protecting and verifying all control and data traffic cryptographically, the security attacks can be contradicted. Appropriate trust relationships needs 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. [9]. Secure communication in mobile ad hoc Network is a very important issue because of the active nature of the network topology.

1.3 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 network.
- 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. [10]

MANET security threats can be basically classified as

1. Active attacks where it includes

a) Denial of Service
b) Jamming
c) Masquerade
d) Fabrication
e) Modification

2. Passive attacks that include

a) Traffic Analysis
b) Eavesdropping
c) Network Analysis

Apart from the usual threats, achieving security within ad hoc networking is challenging due to following reasons: Wireless Environment, Absence of Central authority, Selfish Nodes, Dynamic Topology, Limited Computational Capability [11].

1.4 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. [11]

1.5 Problem Identification and Proposed Solution

In our proposed work, we will design 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. We use a reactive certificate distribution mechanism using multiple Certificate Authority node. Nodes trusting and being trusted by more than one Certificate Authority should apply for certificate. A node without a certificate or needing to renew his certificate must ask to other nodes in the mobile ad hoc Network for a certificate issuing.

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

1) Any one of AUTH and INTEG
2) All of AUTH and INTEG
3) AUTH and INTEG

where 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.

II. Related Work

Alan J. Ford et al [12] have discussed the problems arising from dynamic connectivity between heterogeneous MANETs and external networks, and details future research plans to provide routing between disparate systems based on metrics including bandwidth, latency, cost, and user requirements.

Mansoor Alicherry et al [13] 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.

Mrs. Sugandha Singh et al [14] have made the traditional approach to security inadequate. With this view in mind decentralized group key management is taken into consideration. A novel structure of the node is proposed and each entity holds a secret share SSi of each node in 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 network considered is not very highly volatile. So we have to investigate the group key management for highly volatile network.

Wenjia Li et al [15] 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.

Yuu-Heng Cheng et al [16] 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.

N.Jaisankar et al [17] have proposed a novel agent based framework to monitor, detect, and isolate misbehaving nodes in the MANET. The proposed framework protect 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.

III. Proposed Work

3.1 Trust based packet forwarding scheme

We introduce a the scheme for the purpose of data security. We calculate the trust index using the Algorithm 1 and the Route is selected based on the trust Index of all nodes.

3.1.1 Trust Index Calculation

Let

$Z = \{N_1, N_2, \ldots Nn\}$ be the network of nodes.

T_i be the trust index of node N_i,

T_{inc} be the value of trust increment,

T_{dec} be the value of trust decrement,
T_{th} be the trust threshold value.
N_k be the node which forwards a data packet P_k.
p be 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
   Node i decrements trust index of N_k by
   $T_{dec} = T_{dec} - 2*p$
   Compare T_{i-1} with $T_{th.}$
   If $T_0 < T_{i-1} < T_{th}$,
   Packet is dropped.
   Else
   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 increments trust index of N_k by
$$T_{inc} = T_{inc} + p$$
End if

End if

3.2 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
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

1. 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.
   Else if Tr(A) = Tr(B), then
   If $N_{hi}^A > N_{hi}^B$
   Select N_{hi}^A
   Else
   Select the shortest route.
   End if
   End if

3.3 Distribution of Certificate Authority among Cluster Heads

- Initially each node calculates its trust index using the above method. Each node gets the trust value from 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 shareholding DCA nodes.
- The CH can satisfy this role since it holds the positions of responsibility and has direct communication with one other.
- Distribution of the DCA private key is processed and it is maintained among the cluster heads. A share of the DCA private key needs 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 $\{1, \ldots, b-1\}$.

3.3.1 Bootstrapping

Let, C be the initial set of CHs at 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 $e_i = sv_i \bmod a$.

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 $f_i(0) = v_i \bmod u$

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 $e_{i,t} = s^{vi} \bmod a$. The consistency of the subshares are verified by these values and are sent by CHi. Let $Et = \prod_{i \in C} e_{i,t}$, where t €{0 . . . r-1}

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

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

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 $dj = \sum_{i \in C1}$ fi(j)

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

3.3.2 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.

$e = s^d \bmod a$.

(a,b,s,e) = Public key.

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

1. $\rho = (s^w \bmod a) \bmod b$;
2. $\psi = \rho l + w\eta \bmod b$;

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

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

The following (m,l) threshold signature scheme based upon the prior variant of DSS, is assumed here Let C2 $\subseteq$ C1 (where $|C1| \geq m$) be 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 for 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.

$\mu = s^w \bmod a$

$\rho = \mu \bmod b$

$H_t = \prod_{i \in C3} s^{hi,t}$

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

$$s^{\psi t} = (e \prod_{j=1}^{m-1} (Ej)^{tj}) \rho (\mu \prod_{j=1}^{m-1} (Hj)^{tj})^{\varepsilon(REQ)}$$

Using lagrange formula to {ψi}, ψ can be computed by the requesting node

$$\psi = \sum_{j=1}^{m} \prod_{q \neq j} i_q / (i_q - i_j) \text{ for any } CH_{i1}, \ldots\ldots CH_{ik} \in C3$$

3.3.3 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 updation.
- If the node doesn't receive initialization messages, at the end of the backoff period, the node sends 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 updation 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 collision increases, but it leads to prolonged backoff 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 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.

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 have updated their shares at the end of the update procedure. The remaining CA nodes in the network are updates 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.

Depending upon the nature of data and users requirements, user policies(P) can be specified which can take the following values.

I only Integrity

A only Authentication

IA both Integrity and Authentication

Based on the policy of the user, the corresponding security modules can be executed as per the following algorithm.

Algorithm 3

If Policy = I then

Calculate the Trust Index of all the nodes according to the algorithm 1 in section 3.1.1

Select appropriate route using the algorithm 2 in section 3.2.2

Else if Policy = A then

DCA private key is applied to deliver security service according to section 3.3.2

Share updation is done among the cluster heads according to section 3.3.3

Else if Policy = I and Policy = A then

Calculate the Trust Index of all the nodes according to the algorithm 1 in section 3.1.1

Select appropriate route using the algorithm 2 in section 3.2.2

DCA private key is applied to deliver security service according to section 3.3.2

Share updation is done among the cluster heads according to section 3.3.3

End if

IV. Simulation Results

4.1 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 meter x 500 meter region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the number of attackers is varied from 2 to 10. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1

No. of Nodes	50
Area Size	1500 X 500
Mac	802.11
Radio Range	250m
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

4.2 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.

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

The simulation results are presented in the next section. We compare our PB-CDS protocol with the PB-DGKS [10] protocol in presence of malicious node environment.

4.3 Results

Based On Attackers

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

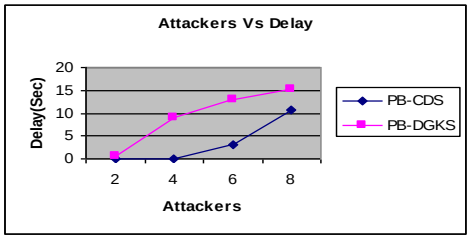

Fig 1: Attackers Vs Delay

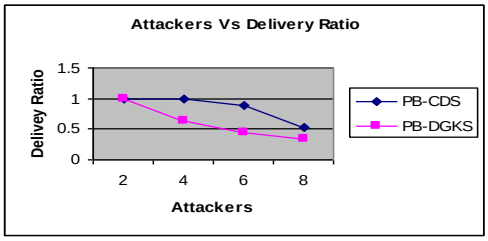

Fig 2: Attackers Vs Delivery Ratio

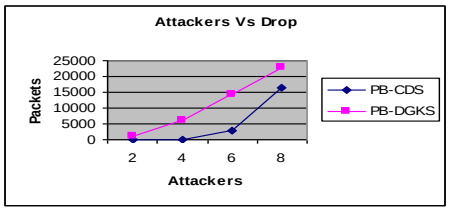

Fig 3: Attackers Vs Drop

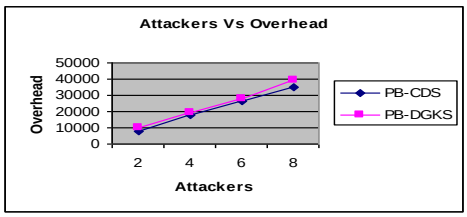

Fig 4: Attackers Vs Overhead

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 show the results of 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.

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.

V. Conclusion

In this paper 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 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 a 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

[1] I Shin, YShen, Y.Xuan, "A Novel approach against reactive attach" Ad hoc and sensor Wireless Networks VOL.0,1-25,2010

[2] P.Papadimitratos , ZHass, "Securing Mobile Ad hoc Networks " The Handbook of Ad Hoc Wireless Networks, M.Ilyas, Ed. BocaRaton: CRC Press 2002 pp. 31.1-31.17.

[3] H.Yang, H. Luo, F. Ye, S.Lu and U. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions ", IEEE Wireless Communications, Vol. 11,no. 1 Feb.2004, pp.62-67

[4] Ljubica Blazevic, Yves Le Boudec. "A Location-based Routing for Mobile Ad Hoc Networks". IEEE Transactions on Mobile Computing Vol. 4, No. 2., March 2005 pp 97-102

[5] S.Dhanalakshmi and Dr.M.Rajaram "A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET**"** IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008

[6] Bhavyesh Divech Ajith Abraham, Crina Grosanand Sugata Sanyal "Impact of Node Mobility on MANET Routing Protocols Models" Journal of Digital Information Management, 2007.

[7] Alexander Nouak "MANET Security" Sixth International Conference on Intelligent Information hiding and multimedia signal processing "October 15-17, 2010 in Darmstadt, Germany.

[8] Nishu Garg and R.P.Mahapatra **"**MANET Security Issues" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009

[9] Panagiotis Papadimitratos and Zygmunt J. Haas "Secure message transmission in mobile ad hoc networks" Elsevier B.V. Ad Hoc Networks 1 (2003) 193–209

[10] Ovais Ahmad Khan "A survey of Secure Routing Techniques for MANET "Course Survey Report, fall 2003.

[11] Aniruddha Chandra "Ontology for MANET Security Threats" Proc. NCON, 2005.

[12] Alan J. Ford and Jon Crowcroft "Applying Policy to Inter-domain MANET Routing in Challenging Environments" Proceedings of the Second Annual Conference of the International Technology Alliance, LondonUK, Sep 2008.

[13] Mansoor Alicherry , Angelos D. Keromytis1 Angelos Stavrou2 "Deny-by- Default Distributed Security Policy Enforcement in Mobile Ad Hoc Networks" 5th International ICST Conference on Security and Privacy in Communication Networks, 2009.

[14] Mrs. Sugandha Singh, Dr. Navin Rajpal, Dr. Ashok Kale Sharma and Mrs. Ritu Pahwa "Policy based Decentralized Group key Security for Mobile Ad-hoc Networks**"** IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 10, May 2010.

[15] Wenjia Li, Anupam Joshi, and Tim Finin "Policy-based Malicious Peer Detection in Ad Hoc Networks" 2009.

[16] Yuu-Heng Cheng, Abhrajit Ghosh, Ritu Chadha, and Gregory Hadynski "Managing Network Security Policies in Tactical MANETs Using DRAMA" 2010 IEEE

[17] N.Jaisankar, R.Saravan and K.Durai swamy "An agent based security framework for protecting routing layer operations in MANET" First International Conference on Networks & Communications, 2009.

[18] Andel T.R. and Yasinsac A., "Surveying Security Analysis Techniques in MANET Routing Protocols," IEEE Communication Surveys & Tutorials, vol. 9, 2007, pp. 70-84.

[19] Tara M. Swaminatha and Charles R. Elden, "Wireless Security and Privacy: Best Practices and Design Techniques," Addison-Wesley,2009

About Authors

Mr. L. Kartheesn obtained his Bachelor's degree in Computer Science and Engineering from University of Madras in the year 1994 at Chennai, Tamil Nadu, India. He obtained his Master's degree in Computer Science and Engineering from University of Madras in the year 2000 at Chennai, Tamil Nadu, India. Currently he is pursuing his PhD in the field of Network Security at Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV University), Kanchipuram, Tamil Nadu, India. He is Life Member of the ISTE. Currently, working as Professor & Head in Department of Computer Science and Engineering at Adhiparasakthi College of Engineering, India. He is specialized in Computer Networks, Cryptography and Network Security and Information Security He has presented papers in conference and participated actively in different discussion forum His current research interests are Security in Networks based on Policy and procedure and mobile adhoc Security.

Dr. S.K. Srivatsa born at Bangalore on 21st July 1945. He received his bachelor of Electronics and Telecommunication Engineering from Jadavpur University, Master degree in Electronics Engineering & Ph.D both from Indian Institute of Science, Bangalore. He retired as Professor of Electronics Engineering from Anna University in July 2005. Since Aug. 2005 he is Senior Professor in St. Joseph College of Engineering, Chennai. He is a life fellow, member in about two dozen Professional Society. He is the author of over five hundred Publications. He has produced 34 PhDs. He is a recipient of about dozen Awards. His research interests pertain to Computer Networks, Digital Logic, Design & Analysis of Algorithm and Robotics.