ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Methodology of Producing Security in AD HOC Networks Using Identity and Trust Key

S.Divya
PG Scholar,
CERD, Department of Electronics and Communication Engineering
Mallareddy Institute of Engineering and Technology, Secunderabad, India.

Mr.M.Naresh, M.Tech
Assistant Professor,
CERD, Department of Electronics and Communication Engineering
Mallareddy Institute of Engineering and Technology, Secunderabad, India.

Prof. Dr.M.Narsing Yadav, Ph.D
HOD,
CERD, Department of Electronics and Communication Engineering
Mallareddy Institute of Engineering and Technology, Secunderabad, India.

Abstract:
Communication in Mobile Ad hoc network is done over shared wireless channel with no Central Authority (CA) to monitor. Responsibility of maintaining the integrity and secrecy of data, nodes in the network are held responsible. To attain the goal of trusted communication in MANET (Mobile Ad hoc Network) lot of approaches using key management has been implemented. This work proposes a composite identity and trust based model (CIDT) which depends on public key, physical identity, and trust of a node which helps in secure data transfer over wireless channels. CIDT is a modified DSR routing protocol for achieving security. Trust Factor of a node along with its key pair and identity is used to authenticate a node in the network. Experience based trust factor (TF) of a node is used to decide the authenticity of a node. A valid certificate is generated for authentic node to carry out the communication in the network. Proposed method works well for self- certification scheme of a node in the network.

Keywords:
MANET, Trust Model, Certificate, Public key, Secret key.

INTRODUCTION:

Ad hoc networks are infrastructure less networks with every node equipped with processing capability and acting as a router for other nodes. Nodes in such networks believe on intermediate nodes for routing the data from one end to the other.

As ad hoc network are wireless and all transmissions are done on the fly, they're prone to varieties of routing attacks. Communication within the network depends on the nodes and at any point of time the danger of a node being compromised exists. Ad hoc networks have several advantages like a node can be added simply to a network, no geographical limitations, no need to modify the present surroundings for accommodating new nodes [1] and many more however at the same time as it is infrastructure less, communication is on the air, no central authority, dynamic topology: security is hard to attain. A key advantage of ad hoc networks over standard networks is that ad hoc network has no single point of failure [2]. For attack free transmission trust among the nodes has to be established so the communication can be done through the most trustworthy node.

To scale back the impact of non-trusted nodes and attain the next level of security this work proposes a composite identity and trust based model (CIDT) that relies on TF (Trust Factor) and ID (Identity) of a node to ensure security of the network. Key generation and distribution that are necessities of PKI security is tough to be enforced among MANET that lacked trust authorities. Therefore the notion of relative security may be adopted for MANET. In this work a CIDT model modifying the classical DSR routing protocol has been proposed that relies on PKI and the trust factor of a node to designate it as a valid or invalid node.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

This trust factor is computed on the basis of the total number of successful transmissions done by a node.

RELATED WORK:

Certificate-based public key management approaches need public keys to be distributed wherever the receiving party ought to be able to authenticate the received key, based on the certificate of the public keys. Thus, a trustworthy CA is needed to deal with key management operations as well as key generation, distribution, revocation, and update [3]. For MANETs without trustworthy CAs, certificate-based approaches ought to operate in a very self-organized manner. Capkun et al. [4] proposed a certificate-based public key management where every node generates problems pairs of its own public and private keys and also the certificate of the public key with a restricted validity period thus as to deal with network partitions in MANETs. Chang and Kuo [5] proposedtwo-step secure authentication protocol for multicast MANETs, so as to affect key management.

They used the most trustworthy node as a CA and also the second highest trustworthy node as a backup CA. Huang and Wu [6] proposed certificate path discovery algorithm for MANETs based on the hierarchical PKI structure using multiple CAs with no specific trust framework given. Huang and Nicol [7] proved that the shortest certificate chain doesn't guarantee the most trustworthy path to get the public key of a target node due to totally different trustworthiness observed in every intermediate node on the certificate chain. Vinh et al. [8] propose a group header for public key management in a group communication system. Group header is selected based on the trust.

Shamir [9] uses the construct of ID-based public key management scheme that generates a public key supported the ID of the node (e.g., IP or email address) and itscorresponding private key generated by a trusted CA. In threshold cryptography [10], the private CA key is distributed over a group of server nodes through a (k, n) secret sharing scheme.

The key is CA secret is shared between n nodes in such a way that trusted k nodes should collaborate so as to reveal the key. However, a central trusted authority exists to choose the servers among whom they must be shared and distributes the key.

PROPOSED MODEL:

Most of the work discussed in section 2 relies on key pair for achieving security. A key pair of a node may be compromised and it becomes tough to detect it due to mobile nature of a node in ad hoc network. There is a possibility that a node which exhibited malicious behavior might have moved out of the range to detect / monitor its activities. A malicious node may also generate a key pair and may propagate it in the network and may harm the network resources. A trust factor of a node combined with the identity of a node encrypted using the secret key of a node may prove to be a good solution. It will prove to be a strong system as the keys of only the trusted node will be authentic and verified during transmissions. Certificates will also be generated only for valid keys of trusted nodes. This work proposes a composite identity and trust based key management model which helps in improving the performance of the nodes in the network.

A. Trust Model:

Trust Factor of a node depends on how successfully it transmitted the data during its lifetime. The total successful and unsuccessful transmissions are judged by the total number of packet dropped by the network and every node in the network. Total packets dropped by a node decide its trust Factor. The TMS (Trust Management system) in [11] is used to evaluate the trust factor of a node. Direct trust model and recommended trust model has been used for evaluating trust. Trust of a node a on another node b trying to enter the network can be defined as a function of two parameters as given in equation (1).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

B. Composite Identity and Trust based Model (CIDT)

CIDT is a composite identity and trust based model that depends on the identity of a node along with the trust factor of a node in the network. A node in the network is identified by it physical identity and its key pair. The sub processes that are executed in CIDT are key generation, certificate computation; public key distribution and key revocation detailed briefly in the upcoming sections.

$$TF_{a,b} = DTF_{a,b} + RTF_{a,b} \qquad (1)$$

Where

$TF_{a,b}$ → Trust of node a on node b.
$DTF_{a,b}$ → Direct Trust Factor of a node a on node b and it is computed by a by directly monitoring the b.
$RTF_{a,b}$ → Indirect Trust Factor of node a on node b which is computed after getting the trust level of b from its 1 hop neighbor nodes.

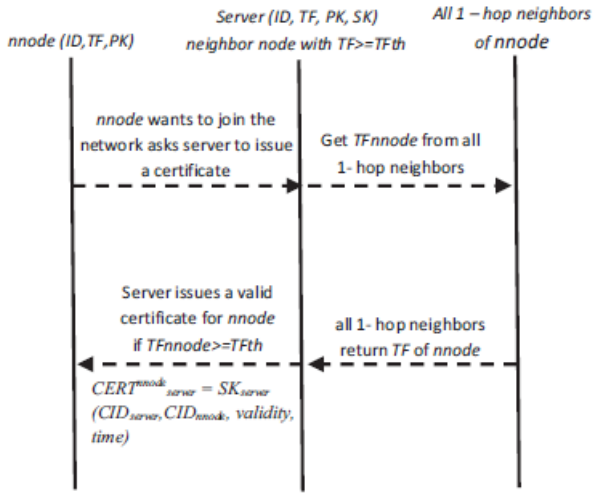

Figure 1: Certificate Computation for *nnode*

a) Key Generation:

Every node in the network generates a key pair (PK,SK) for authentication and it is updated periodically. Before distributing a key pair in the network, a node should be able to acquire the certificate of the public key from a trustworthy node. Node in the network is identified by its Public Key (PK), its identity in the network (ID) and Trust Factor of a node in the network (TF).

b) Certificate computation for new node (nnode):

When a new node nnode trying to join the network it sends its ID to the server node for issuance of certificate to it for being a part of the network. The server node verifies the validity of the requesting node by checking for its TFth (Trust FactorThreshold) with the neighbors. Validity is a trustcertificate issued to a node by its neighbor on successful verification. Validity factor between two nodes x and y is validity (CIDy) is the confidence of x that y is authenticparty. A node can be either an invalid or a valid node.

$$CERT^{nnode}_{server} = SK_{server}(CID_{server}, CID_{nnode}, validity, time) \qquad (3)$$

Where CID of *server* and *nnode* can be further decomposed using equation 1.

$CERT^{nnode}_{server}$ – *certificate computed by server for nnode.*
SK_{server} - *Secret key server node*
CID_{server}- *Composite Identity of server node*
CID_{nnode} – *Composite identity of nnode*
Validity – Validity of certificate
Time – time period for which this certificate remains valid

Public Key Distribution:

After a node obtains its public key certificate, it periodically disseminates its public key with the certificate to all of its 1-hop neighbors who are trusted. When a node nnodedisseminates its public key and the certificate to the set of 1-hop neighbors, the packet consists of the following items:

$$(SK_{nnode}(CERT^{nnode}_{server}), PK_{nnode})) \qquad (4)$$

$CERT^{nnode}_{server}$is the certificate of nodennodes' public key signed by the servers' secret key including the information of the nnode ID, the server's ID, the validity if CERT and expiration time for the certificate of the public key. SK nnodeisnodennodes' secret key, and PK_{nnode}isnodennodes' public key.

d) Key Revocation and Update:

The secret / public keys of a node will be revoked after the validity period expires. Since the certificate includes the information of expiration time, key revocation due to the passed valid period will be implicitly known to other nodes in the network. Keys

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

can also be revoked if they are found compromised.

e) Node Authentication:

A node is authenticated if it is a valid node of the network. Below given is the algorithm which authenticates a node.

```
n node in the network
N Set of all nodes in the network
For all node n ∈ N
        Check the validity of the CERT^n_server
        If CERT^n_server is valid
                then Authenticate node n
        else
                Declare node n as unauthentic
                entity
Broadcast this message in the network.
```

Simulation Results:

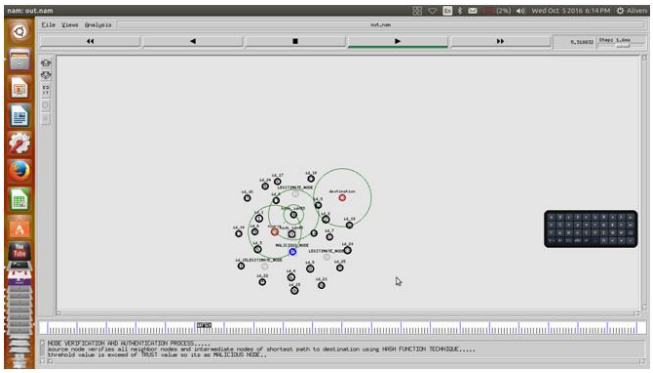

Fig: NAM

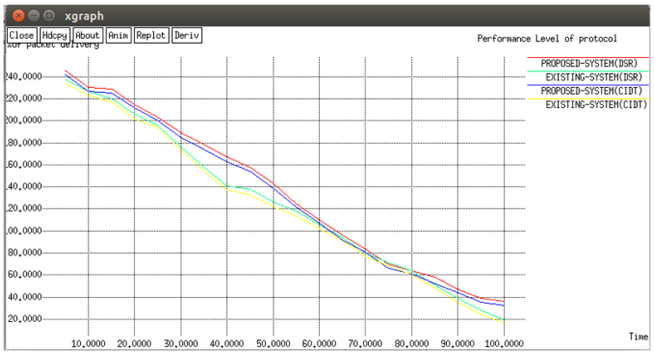

Fig: performance level protocol graph

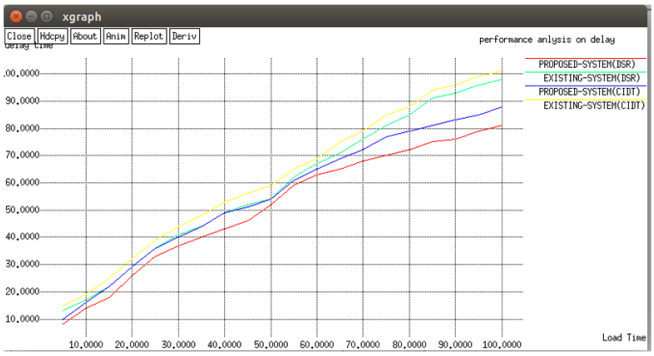

Fig: performance analysis on delay

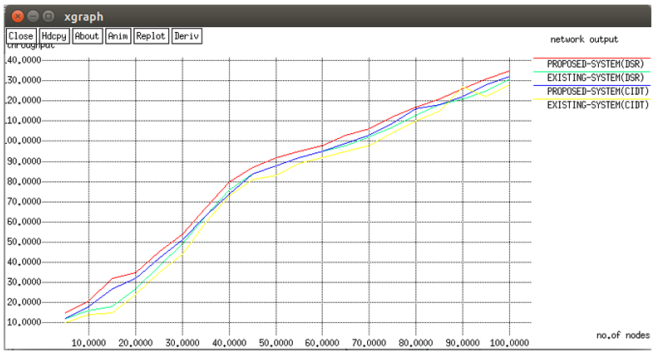

Fig: network output

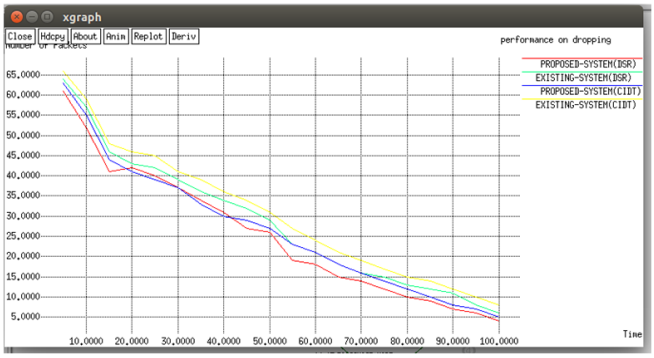

Fig: performance on dropping

CONCLUSION:

In this work key management techniques applied to MANET to achieve secure transmission are being analyzed. Key management algorithms use cryptography, certificate schemes, certificate validity for attaining a secure network. This work has put forth a model which along with the key pair of a node depends on trust factor of a node to issue s certificate and authenticate a node. Our analysis proposes enhancements like usage of trust factor of nodes while choosing a node.

Throughput of the network and Packet Delivery Ratio in the network is enhanced by this algorithm.

REFERENCES:

[1]C.E. Perklins, "Ad Hoc Networking", 1st edition. Addison –Wesley Professional, 2001.

[2]I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, Volume 47, 2005, pp. 445-487.

[3]H. Dahshan, and J. Irvine, "A trust based threshold cryptography key management for mobile ad hoc networks," IEEE 70th Vehicular Technology Conf., Anchorage, AK, USA, pp. 1-5, Sept. 2009,.

[4]S.Capkun, L. Buttya, and J.-P. Hubaux, "Self organizedpublic-key management for mobile ad hoc networks," IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan. – Mar., 2003.

[5]B.J. Chang and S.L. Kuo, "Markov chain trust modelfor trust-value analysis and key management in distributed multicast MANETs," IEEE Transactions on Vehicular Technology, vol. 58, no. 5, pp. 1846-1863, May 2009.

[6]He Huang ,Shyhtsun Felix Wu, An approach tocertificate path discovery in mobile Ad Hoc networks, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, October 31, 2003, Fairfax, Virginia

[7]J. Huang and D. Nicol, "A calculus of trust and its application to PKI and identity management," ACM 8th Symposium on Identity and Trust on the Internet, Gaithersburg, MD, USA, April 2009.

[8]N. V. Vinh, M.-K. Kim, H. Jun, and N. Q. Tung, "Group-based public-key management for self-securing large mobile ad-hoc networks," Int'l Forum onStrategic Technology, pp. 250-253, Oct. 2007.

[9]A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," CRYPTO'84, 1984, pp. 47–53.

[10]Y. G. Desmedt, "Threshold cryptography," European Transactions on Telecommunications, vol. 5, no. 4, pp. 449-458, July/Aug. 1994.

[11]Khatri, P., Tapaswi, S. &Verma, U.P. (2012). Trust evaluation in wireless ad hoc networks using fuzzy system. In V. Potdar& D.