The New Approach to provide Trusted Platform in MANET

Renu Dalal[1#], Manju Khari[1] and Yudhvir Singh[2]

[1]Department of Computer Science & Engineering, AIACTR, New Delhi, India
dalalrenu1987@gmail.com
[2]Computer Science & Engg. Dept, U.I.E.T M.D University, Rohtak, India
yudhvirsingh@rediffmail.com

ABSTRACT

In distributed operation, we uses different key management schemes, authentication and many trust models, but in wireless medium having reliability problem, hidden terminal problem etc. To provide authenticated nodes and secured environment is the important issue in MANET. Frequent path breaking, multihop wireless link between mobile nodes, self organization and maintenance are such properties that makes difficult to provide trust in MANET. This paper proposes the new trust scheme, which provides malicious free atmosphere for mobile ad-hoc network. This model first check the authenticity of nodes through challenge response method and then PKI certificate will be given to only authenticated nodes so as to enable the trusted communication platform. At last this paper give the comparisons of ACTP model with other existing trust model.

Keywords

TTP, MANETs, PKI, Symmetric key Cryptography, Trustworthiness, Multihop.

1. INTRODUCTION

In mobile ad-hoc network having many security breaches, to avoid these breaches we have to implement security policies like integrity, confidentiality and authentication MANET is the infra-structreless network which consists of mobile nodes and performs their various functions in a random period of time. To perform the correct operations in network, role of router, server and client will does by mobile nodes [1]. Because of economically less deployment of MANET, we find its applications in different areas like military, battlefield, emergency operations and collaborative computing. MANET does not consist of centralized control so this network is highly vulnerable to various kind of attack. For communication in MANET it includes two basic steps 1. Route Discovery 2. Data Transmission and both steps can be easily attacked by the attacker [2].

To achieve the high security in MANET lots of trust schemes and key management schemes have been used.In MANET attack can be classified as Active and Passive attack. If the attacker

does the passive attack, it is undetectable because attackers will only sniffing the packets which is being transmitted over the network from one mobile node to other. In active attack, attacker can temper the packet/ packets, misleading the nodes in network, but this type of attack can be easily identified. To provide security and prevention from different vulnerabilities in MANET, the trust model which ensures that malicious node can't enter in network and hence creating a secure environment for communication is proposed.

This paper, proposes the new trust model for MANET, that achieves high security level for mobile nodes and only trustworthy nodes can enter in network. This model using the concept of challenge response to find the authenticity of node and provide certificates to trustworthy nodes .This paper organized as: section 2. Will gives knowledge about related work. The proposed work ACTP model will be discussed in section 3. In section 4, Expected analysis of ACTP model is discussed. Section 5 presents conclusion of the paper & its future work.

2. RELATED WORK

In this section, the base of idea working behind ACTP model is discussed. Group key management concept used by Wu, B [3] in 2007. In this model TTP (trusted third party), key distribution centre (KDC) is used. KDC generates and distributes secret key to group member and TTP shares a group key (secret key) to group member. LKH (local key hierarchy) model were proposed by [4, 5]. This model using hash function and efficient key tree structure, root node of the tree will works as GKC (group key controller) i.e. TTP and tree's leafs will be as group member because of using one way function tree(OFT). The keys generated in LKH model are totally different with each other. Group key management and LKH model only can be applied for those network which having centralized/ fixed infrastructure, but MANET is dynamic network in which any node come and join the network & also leaves the network at random period of time [6]. GDH.3 and BD are those models which use the concept of group key management and designed for dynamic network [7, 8]. The GDH.3 protocol model work on any node will together past experience from all input. In this model, node take O (n) exponentiation at last broadcast the result value to the remaining group. In BD protocol model, Diffie Hellman (DH) protocol is used, neither of computing nested computations. Another scheme is introduced by KIM [9], it is called TDGH. This scheme used concept of DH and efficiency of key tree structure.

Hybrid Group key management architecture for Heterogeneous MANET was purposed by WEI-Chu-Yuan in 2010 [10]. This model used hierarchical state routing (HSR), LKH and TDGH protocol in cluster and nodes of cluster head, who is responsible for management in Heterogeneous MANET. Cluster head node generates the group key and distributes it to small group of mobile nodes i.e. clusters, who shares same group key. The special feature of this model, there is no need to key updating of ordinary node.

Public key certificate management for mobile ad-hoc network was disclosed by P.Caballero and C.Goya in 2010. The combination of MPR (multi point relay) and MDA algorithm used in this model for utilizing the smallest no of certification chain to reach the rest of mobile nodes. The special feature of MPR-Gout heuristic [11]:-no need of communication between mobile nodes, while doing authentication and verification procedure. High certificate rate considered and shortest certificate chain is generated in this model.

3. PURPOSED ACTP MODEL

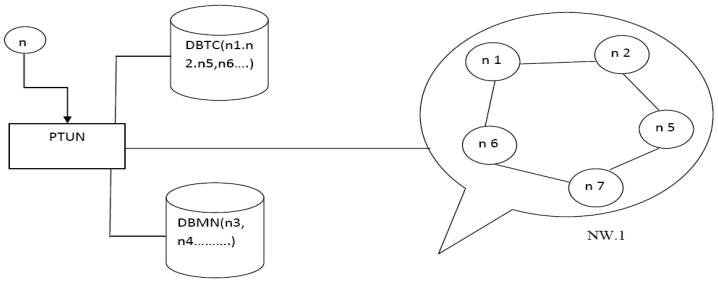
Providing secure communication between mobile nodes, decreasing overhead, location update and updating locations are such issues in manet which provides unsafe atmosphere in manet.. Mobile ad-hoc network is a network that creates self organized and efficient environment of nodes to provide communications and various kinds of operations between them. To maintain the trust between mobile nodes and to make the malicious free atmosphere in MANET, the new trust model for mobile ad-hoc network. Authenticity Check to provide Trusted Platform (ACTP) in MANET takes the concept of challenge & response by using symmetric key cryptography user authentication (UA) second approach [12], in which ACTP model test the trustworthiness of each node that want to join the network and then provided the PKI certificate (X.509) to trustworthy node for showing the authenticity of node. The working of symmetric key cryptography, user authentication second approach is briefly explained in the working of ACTP model second step. User authentication second approach takes three steps to find that the node is trustworthy or not. For providing certificates this model using self organized approach of PKI [11], in which model maintains minimum number of certificate chain.

Version	Serial No.	Signature	Issuer	Validity period	Subject Name	Node ID

Header Format (X.509)

Figure 1

For testing the trustworthiness of each node PTUN unit using user authentication (UA) second approach of symmetric key cryptography and for showing the authenticity of every node, each node maintains the self chain of certificates by using self organized approach of PKI. In self organized approach of PKI, each node having the header format, that contains version, serial number, signature, issuer, validity period, subject name, and node id. Each node having their own different id that shows the authenticity of individual node, this id is provided by primary test unit of all nodes. Header Format which is maintains by every node is shown in figure 1.In header format last field of X.509 that is public-key is replaced by node id because it reduces the overhead on the node. Table 1 defines different key terms which are used in ACTP Model with their definition.



OVERVIEW OF ACTP MODEL

Figure 2

Key Terms	Definition
1. n (mobile node)	Here, n defines the any mobile node that wants to enter in NW.1 (network).
2. PTUN (Primary Test Unit for all Nodes)	This unit will test the trustworthiness of each mobile node and provide the PKI certificate (X.509) for authenticity of node. Average trust value is calculated and removal of malicious node is done by PTUN.
3. DBTC(Database for Trustworthy Nodes)	DBTC is the database, which stores the information about those mobile nodes who is trustworthy (for example node n1, n2, n5, n6, n7 are trusted nodes).
4. DBMN(Database for Malicious Nodes)	This is database for those mobile nodes that is not trustworthy and fails in the test, which is performed by PTUN (for example node n3 and n4 are malicious nodes).
5. X.509	X.509 is a protocol that defines the structure of certificate in a systematic way. It is consisting of different fields but last field (public key) is replaced by node id field (for ACTP Model).

Table 1

3.1 WORKING OF ACTP MODEL

Step 1:- Initially network nw.1 is empty at while there were no node want to come in this network. PTUN is existing and DBTC, DBMN database are kept empty.

Step 2:- If any node wants to join nw.1 PTUN will test node's authenticity by giving to challenge that node.

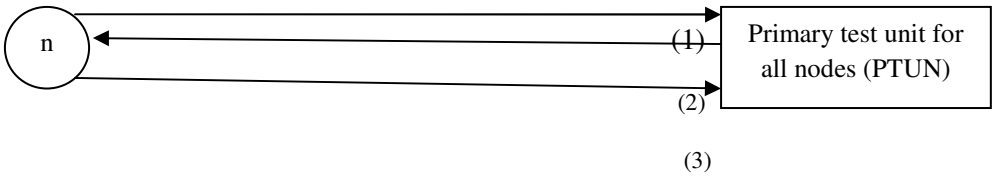


Figure 3

(a) PTUN unit using symmetric key cryptography (user authentication 2nd approach) [12].

(b)Working of user authentication 2nd approach is shown in figure 3.

(1) Node sends their identity (in plaintext) to PTUN.

(2) PTUN challenge node by sending a nonce, Rb, in plain text.

(3) Node responds to this message by sending back nonce and encrypting it by using symmetric key [12]

Step 3:- If that node proves their authenticity, then X.509 Certificate will be provided to that node. This TC (trust certificate) will be store in DBTC .By using chain of certificates (self organized approach), in which nodes receives their certificate by PTUN (node).

Step 4:- If the node is not authentic and fail in their response which is sends to PTUN, that node will be declared as malicious node .All information about this node will be stored as DBMN.

Step 5:- After making or constructing the network nw.1, every node generates TRAN (Trust Report for All Nodes) in any random period of time. After making TRAN, all nodes will be submitted it to PTUN.TRAN is based on the interaction between nodes, for example node n 1 generates following TRAN i.e table 2:-

Node Name (NN)	Trust Value (TV)
n2	1
n5	-1
n6	0
n7	1

Here, 1= complete trust.

-1=complete distrust.

0= no interaction.

TRAN by n1 Table 2

Step 6:- Average trust value of each node will be calculated by PTUN and distrust node (MN) will be removed from nw.1, this node come to DBMN.

Step 7:- Nearest neighboring node will be connected to each other. For example n7 is malicious node (MN), then it is removed and node n5 & n6 will be connected (from figure 2).

4. EXPECTED ANALYSIS OF ACTP MODEL

NW.1 is made up of different nodes in which some nodes are trustworthy and some of the nodes are malicious. DBTC stores information about trusted nodes and information about distrust nodes are stores in DBMN. Assume the following terms: Trusted nodes = n1, n2, n5, n6, n7.

Malicious nodes = n3, n4, n8. Here, NW.1 constructing with n1, n2, n5, n6, n7 nodes. Now NW.1 is looks like figure 4. After a random period of time every node makes the TRAN about each node.

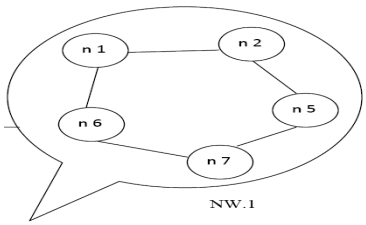
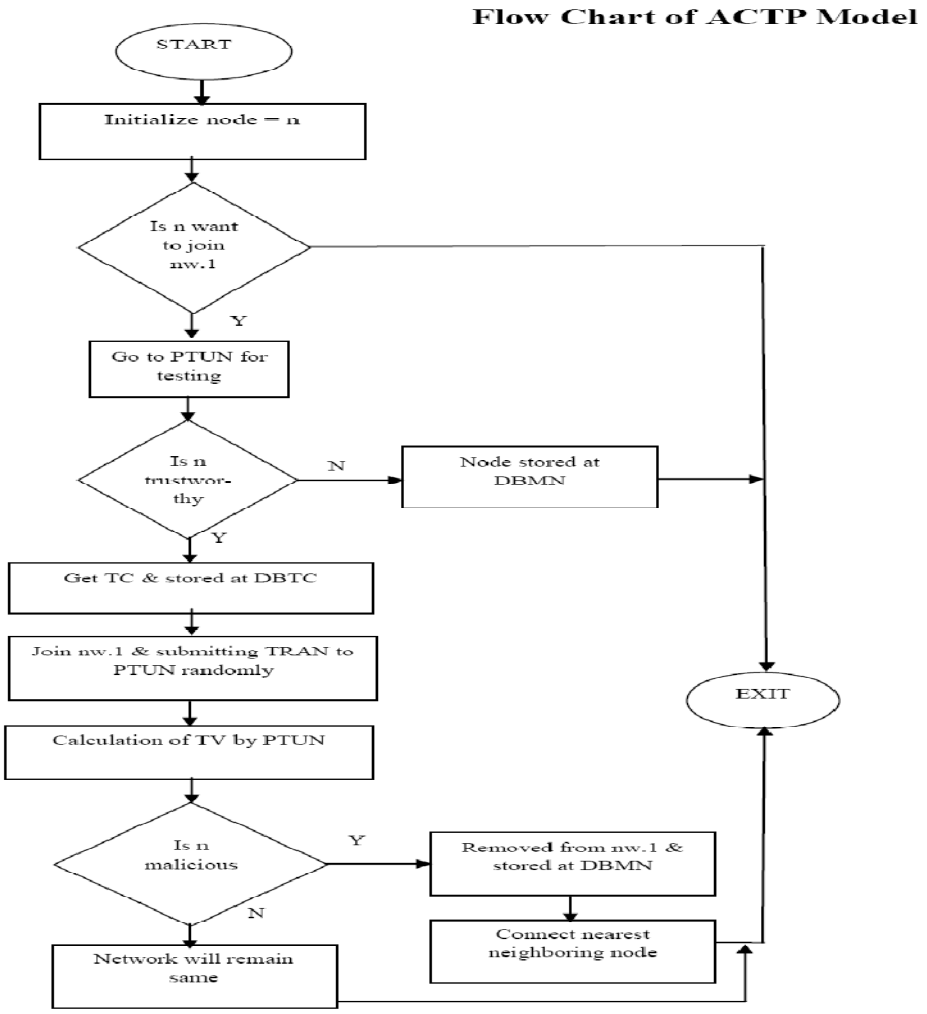


Figure 4



Node Name (NN)	Trust Value (TV)
n1	0
n5	-1
n6	1
n7	1

TRAN by n2 Table 3

Node Name (NN)	Trust Value(TV)
n1	1
n2	-1
n6	1
n7	1

TRAN by n5 Table

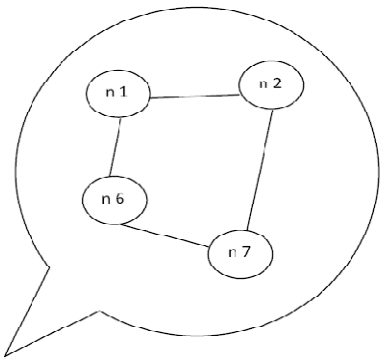
Node Name (NN)	Trust Value (TV)
n1	1
n2	0
n5	-1
n7	1

TRAN By n6 Table 5

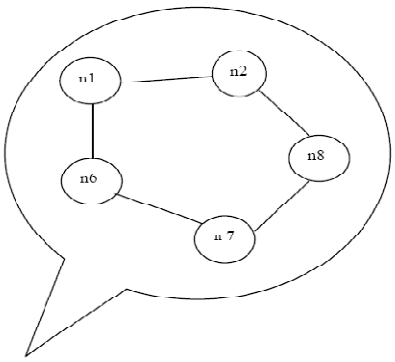
Node Name (NN)	Trust Value (TV)
n1	0
n2	-1
n5	1
n6	0

TRAN By n7 Table 6

After submitting the TRANs by all nodes to PTUN unit, average trust value for all nodes is calculated by PTUN. Now average trust value for n1= 0.5, n2= 0.25, n5= -0.5, n6= 0.5, n7= 1. PTUN remove the node n5 because it having trust value less than 0.Now network NW.1 looks like figure 5. If n8 wants to join network NW.1 ACTP model test their identity and provide certificate to that node if n8 is trustworthy node otherwise information about this node stores in DBMN. Now network NW.1 looks like figure 6.



NW.1
Figure 5



NW.1
Figure 6

5. COMPARISION OF ACTP MODEL WITH OTHER TRUST MODELS

Key Terms	Protocol based	System Level Based	Cluster Based	Maturity Based	PKI Based	ACTP Model
Proposed Year	Before 2000	Between 2000 to 2006	In 2008	In 2010	In 2010	In 2012
Concept	Security Protocols are used	Using Concept of individual level trust model and punishment/reward system	Ad-hoc network is divided into clusters.	Concept of Maturity is introduced for MANET	Concept of Public Key Infrastructure is proposed for MANET	Combination of PKI and Symmetric key cryptography UA 2nd approach
Way of communication between nodes	Indirectly	Directly	[a]Directly with in one cluster. [b]Indirectly (through CH) between two clusters.	Direct	Through Certificates	Through chain of Certificates
Features	1 swaram intelligence, stimergy principle& theory of	1 it can find out selfish node (WATCHDOG) . 2 provide best	1 Zone routing protocol is used 2 trust is calculated by	1 trust increases between people as time goes by,	1 higher level of security is achieved 2 equal work is done by	1 only trustworthy mobile node can join the network.

	simrings is used 2 easily adaptive to mobility 3 solve the problem of dynamic and combinatorial optimization	route link for reliable data (PATHRATER) 3 extracting the nodes which not behaves normally (CONFIDENT) 4 can differentiates selfish and malicious node(CORE) 5 second hand knowledge can't exchanged(OCEAN) 6 using concept of reputation rating(SORI)	using mathematical equations 3 no need of personal and past experiences 4 CH and gateways are used	same concept is used 2 proposed REP protocol 3 using different types of operation modes. 4 no need of authentication 5 trust is calculated by using mathematical equations 6 tolerates up to 35% of liars	nodes in self organized approach 3 centralized CA is used in self organized approach 4 simple bootstrap mechanism & having less maintenance overhead in self organized approach	2 PKI X.509 is used. 3 provides secure environment. 4 simple symmetric key UA 2nd approach is used for find out the trustworthiness of node. 5 DBTC and DBMN database is used.
Types/Examples	ABED,GRE and Trust evidence & evaluation scheme(Other)	CORE,SORI,CONFIDENT etc.	Not exist	Not exist	Self organized and distributed certificate approach	Not exist.
Applicable	Small and large scale of ad-hoc network	Small and large scale of ad-hoc network	Only for small scale of MANET	Small and large scale of ad-hoc network	Small and large scale of ad-hoc network	Small and large scale of ad-hoc network

6. CONCLUSION & FUTURE WORK

This paper addressed the various trust models and key management schemes in MANET. ACTP model for providing trusted platform in MANET is proposed in this paper. This model works on two important concept, first challenge & response for found the authenticity of node, second X.509 certificate for showing trustworthiness of node. This trust model achieves efficient secured platform in MANET. Self organized approach, chain of certificates is used for reducing the overhead of nodes in the network. User Authentication second approach of symmetric key cryptography is used for testing the authenticity of node, this approach is much efficient as compared to asymmetric key cryptography approach. Expected analysis of ACTP model shows that this model can work in efficient way and provides secure atmosphere in mobile ad-hoc network. In future work, we will simulate this model on appropritiate tool and find its disadvantages and solutions for removing these drawbacks.

7. References

1. C.E. Perkins,' Ad Hoc Networking', 1 st edition. Addision- Wesly Professional, 2001.
2. Qiuna Niu, "A Trust-Based Message Encryption Scheme for Mobile Ad-Hoc Networks". Second International Workshop on Computer Science and Engineering, 2009.
3. Wu, B., Wu, J., Fernandez, E., Ilyas, M., and Magliveras, s., 'Secure and Efficient Key Management in Mobile Ad Hoc Wireless Networks'. Journal of Network and Computer Applications (JNCA). Vol. 30, pp. 937-954, 2007
4. Wong, C., Gouda, M., and Lam, S, 'Secure Group Communications Using Key Graphs'. Proc. of the ACM SIGCOMM'98 conference on Applications, technologies, architectures, and protocols for computer communication, pp 68-79, 1998.
5. Wallner, D. M., Harder, E. J., and Agee, R. C., 'Key Management for Multicast: Issues and architectures '. Internet Draft, draft-wallner-key-arch-01.txt, 1998.
6. Renu Dalal, Manju Khari, and Yudhvir Singh, "Survey of Trust Schemes on Ad-hoc Network" CCSIT 2012, Part I, LNICST 84, pp. 170–180, 2012. Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012
7. Steiner, M., Tsudik, G., and Waidner, M.,'Cliques: A New approach to Group Key Agreement'. Proc. of the 18 th international Conference on Distributed Computing Systems (ICDCS'98). Pp.380-387, 1998.
8. Burmester, M. and Desmedt, Y., 'A Secure and Efficient Conference Key Distribution system'. Advances in Cryptology-EUROCRYPT'94, Springer, Berlin. vol. 950. Pp.275-286, 1994.
9. Kim, Y., Perrig, A., and Tsudik, G., 'Simple and Fault tolerant Key Agreement for Dynamic Collaborative Groups'. Proc. of the 7 th ACM Conference on the Computer and Communications Security, pp. 235-244, 2000.
10. WEI Chu-yuan, 'A Hybrid Group Key Management Architecture for Heterogeneous MANET', Second International Conferences on Network Security , Wireless Communications and Trusted Computing, 2010.
11. P. Caballero-Gill and C. Herandez-Goya, "Efficient Public Key Certificate Management for Mobile Ad Hoc Networks," EURASIP journal on wireless Communications and networking, vol. 2011, pp.1-10, 2010.
12. Behrouz A. Forouzen,"3rd edition Data Communication and Networking", Tata McGraw-Hill Publishing Company Limited, 2004.