International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 4, Issue 3, May-June 2015 ISSN 2278-6856

Secure Transmission in MANET using Threshold signature scheme

[1]Jeevan Yadav N S , Sindhu Anand[2]

[1]Lecturer Dept. of Bachelor of Computer Applications Aakash International Business Management College

[2]Research Scholar, Jain University, Bangalore, India

Abstract

The Adhoc network consists of mobile nodes which communicate with each other through wireless medium without any fixed infrastructure. Mobile Ad-Hoc Network (MANET) is a temporary self-organization, autonomous and decentralized infrastructure-free network which provides communication between two or more mobile nodes in situations where environmental constraints are difficult to setup any wired infrastructure and demand totally distributed networks. Due to their wireless links and lack of central administration MANET are vulnerable against adversarial attacks. MANETs have far greater security concerns than conventional networks. MANET must provide various levels of security guarantees to different applications for their successful deployment and usage. As MANET have highly dynamic topology that requires reliability and scalable security mechanisms. Security vulnerabilities in MANETs offer a number of unique properties that offer considerations when determining trust: Self-organization means they are autonomous, with no fixed infrastructure or centralized administrative node. The Proposed work aims at establishing a secure data transmission communication channel using threshold signature scheme. The proposed secure scheme organizes network into clusters using one hop distance and elects the most qualified and trustworthy node as cluster head.

Keywords: - Mobile Adhoc networks, trust value, cluster, cluster head, certificate, threshold signature.

1.INTRODUCTION

A Mobile ad hoc network (MANET) is a collection of resource limited mobile nodes which does not rely on any fixed or centralized infrastructure. These nodes dynamically form a temporary network and communicate with each other through bandwidth limited and multi hop wirelesses links [9]. Clustering is one of the techniques used to manage data exchange amongst interacting nodes. Each group of nodes has one or more elected Cluster head, where all Cluster heads are interconnected for forming a communication backbone to transmit data. Threshold digital signatures are an important cryptographic tool used in most existing key management schemes for mobile ad hoc networks. A threshold-multi signature scheme designed specifically for mobile ad hoc networks allows a subset of shareholders with threshold, to sign an arbitrary message on behalf of the group. The group signature is publicly verifiable and allows any authenticated user to establish the identity of the individual signers. In existing key management proposals for mobile ad hoc networks a distributed certificate authority constitutes the core of the key management services. Threshold signature schemes with traceability guarantee the signature verifier that at least members participated in the group signature and allow the signature verifier to establish the identities of the signers. An important component of any threshold digital signature scheme is the sharing of the group key. The secret share therefore has to be periodically updated to allow only a limited period in which an active and mobile adversary must compromise a sufficient percentage of the shares in order to break the system.

2.SIGNATURE SCHEMES

Mobile Adhoc network security has become a more entangle problem compared to other networks security. In ad hoc networks the nodes often leaves the network and rejoins frequently. So authentication plays a vital role when a node joins and rejoins into the network. A digital signature is another part of the security parameter in the network security. A signature is need in MANET and WSN for detecting the threats and various types of intrusion detection. There are several types of signature schemes used, these schemes helps in identifying the malicious nodes. The signature scheme helps in providing a secure transmission channel for data transmission.

2.1 Different signature scheme in MANET

Signature-based intrusion detection scheme [1] also known as rule-based, it consists of prior stored rules of several security attacks. These rules-based are kept in the database. Signature-based are well suitable for known intrusions, but they are not able to identify the latest security attacks or attacks having no predefined rules. The use of intrusion detection in the traditional wired network is to monitor the network traffic at fixed infrastructure such as routers and switch.

2.2The certificate-based on Public Key

The identity depends on the availability and security of a Certificate Authority, a central control point that everyone trusts [2]. In a MANET, nodes have non-negligible probability to be compromised for the resource limitations of wireless devices and relatively poor physical protection. Once CA is compromised, the security of the network would be subverted. The other obstacle of using Public Key identity in MANETs is the heavy overhead of transmission and storage of Public Key Certificates

2.3 Certificate less Schemes

Certificate less Schemes as a number of features of id based certificate while without having the problem of key escrow. The present a virtual private key generator based escrow-free certificate less public key cryptosystem for MANETs as a novel combination of certificate less and threshold cryptography [3]. In their schemes, virtual private key generators collaboratively calculate the partial private key and send it to the node via public channel. The private key of node is generated jointly by the virtual private key generator and the node itself. Each of them has "half" of the secret information about.

3.TRUST FORMALIZATION

This section mainly describes the trust formalization [8], [6] so that the analysis of Node-based Trust Management (NTM) can be developed. These properties of trust will be defined in later section. In NTM scheme, we need to compute TEs by grasping the TRUSTVALUE from equation 1.Therefore, a node ni's trust on another node nj can be defined as:

$$T_{ni,\,nj} = \alpha_{1ni} T_s^{nj} + \alpha_{2\,ni}\, T^{nj}\, o \quad \ldots\ldots\ldots \text{eqn (1)}$$

In the above equation, T ni, nj is evaluated as a function of two parameters:

i. $_{ni}T_s^{nj}$: Node ni's self evaluated trust on nj ;ni computes this by directly monitoring nj.

ii. $_{ni}\ T^{nj}$ o: Weighted sum of other nodes' trust on nj evaluated by ni.

In eq. (1), α1 and α2 are weighting factors such that α1 +α2 = 1. Thus, by varying α1 and α2, ni can vary the weight of self evaluated vs. others trust in calculating its total trust on nj. Node ni computes this value by directly monitoring nj, when nj is in its radio range. As it mentioned earlier [5] that any node wishes to send messages to a distant node, sends the Route Request (Rtreq) To all the neighboring nodes within the Cluster. The Route-Reply (Rtrep) Obtained From its neighbors are sorted by trust ratings. The source selects the most trusted path. If it's one hop neighbor node is a friend, then that path is chosen for message transfer.

4.CLUSTER FORMATION

After deployment, the nodes broadcast their ID(ni) and TRUST value to their neighbors along with the REQ/REPLY flag[8]. When the participating the nodes have discovered their neighbors, they exchange information about the number of one hop neighbors. The node which has maximum one hop neighbors from the trust interaction table is selected as the TA. Other nodes become members of the Cluster or local nodes. The nodes update the trust values accordingly. A circle is formed with a fixed radius by selecting (either randomly or with highest cooperating neighbor density within 1 hop distance) a node as center and an arbitrary small length as radius. Center of the new circle is computed as the mean of the points within the circle while the radius in increased by the distance of two successive centers. In this manner Clusters are formed in the network. The entire MANET is hierarchical in nature and following sequence is observed network-group-Cluster-Cluster node.

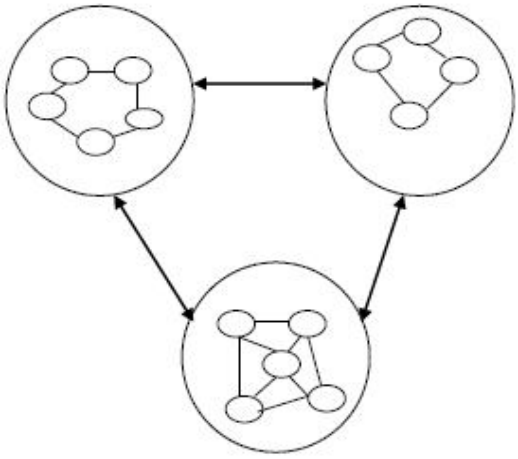

Fig 1: Cluster Formation

Cluster Formation algorithm in NTM
Begin Cluster =1
Repeat
Select a node ni which is 1 hop distance apart from
Other participating nodes with a small length d1
Randomly
Do
N = ni ; d= d1
Draw a circle with ni as center and d as radius
Compute new radius (d1) = d + ni -nj
While ni $\neq$ nj
Cluster-1 is formed with cooperating nodes lying within the circle;
END

5.CLUSTER HEAD SELECTION

In MANET, we denote the set of all nodes as N = n1; n2;:ni where i _ 2. After deployment, pairs of nodes ni; nj € N may interact with each other [8]. Such interaction is regarded as successful if ni and nj both cooperate and denoted as unsuccessful if either of the nodes does not cooperate. The interaction history(IH) of observed outcome between ni and nj , from the perspective of ni, is recorded at any given time t as a tuple:

$$IH_{nij}^{\ t} = (Suc_{nij}^{\ t+}\ U_{nij}^{\ t)}$$

Where $Suc_{nij}$is the number of successful interaction and $U_{nij}^{\ t}$ is the number of unsuccessful interaction between ni and nj .In the node discovery process, which immediately follows deployment, each node periodically, in the order of seconds, broadcasts one-hop hello packets to discover its neighbors. On the reception of a hello message from node ni, node nj replies with an authenticated message using the pair wise key. Embedded in the reply are nj's node ID along with time stamp and location information. If node nj is verified to be authentic, then it is recorded in n neighbors list, and its trust value is initialized.

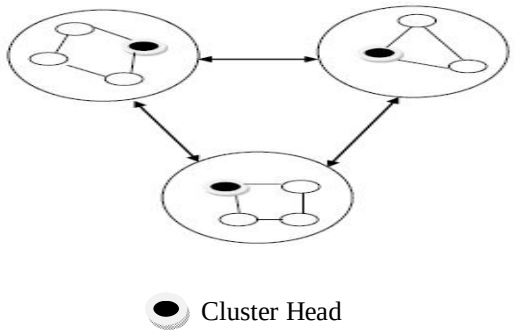

Fig 2: Cluster Head Selection

Cluster head Selection algorithm in NTM
T A_{cur} <— 0
T A_{prev} <— 0
$Time_{prev}$ <— 0
Now () <— 0
Time — OUT_{loop} <— 3*COUNTR
From equation (1) TRUST-VALUE can be further
Evaluated by equation 5
Interaction history (IH) ≥0
While $Time_{prev} \leq$ now() or
TRUST VALUE (TA_{prev}) ≤1 = true do
TA_{prev} remains as Cluster head
end while
if TRUST —V ALUE(TA_{prev}) =
TRUST —V ALUE(TA_{cur}) and
IH(TA_{prev}) = IH(TA_{cur}) then
both TA_{prev} and TA_{cur} remain as Cluster heads
else
select new Cluster head(s)
end if
System Parameter Setup and Individual Self-Certificate Generation
The group members P_i, for i = 1: n agree on and publish the following system parameters:

i. p, q Two large primes, such that q | (p-1).
ii. g Generator of the cyclic subgroup of order q in $(Z)^*_p$.
iii. H(·) One-way hash function.
iv. (n, t) Threshold parameter t and total number of group member's n.
v. T Threshold cryptosystem secret update period.

5.1 Individual Signature Generation
The individual signatures, is based on a variant of the ElGamal signature scheme proposed by Yen et al[13]. It can be shown that this variant is secure against forgery and more efficient to compute than the original ElGamal digital signature. Each node in the cluster is assigned with a signature which is calculated by an algorithm. Which in turn is verified by the cluster head and a list of the entire trusted nodes is made.
Any subset β of t or more members can represent the group and sign an arbitrary message m.
Each member Pi, i€p selects a random integer ki €(1,q -1) and computes $r_i = g^{ki} \mod p$. Each member verifiably encrypts K_i with its own public key PK_i using a verifiable encryption scheme to generate $E_{pki}(k_i)$. Each member broadcasts its ri and cipher text $E_{pki}(k_i)$ to all other members. This implies that each member commits to its public value r_i and provides a knowledge proof of its corresponding discrete logarithm, ki.

5.2Individual Signature Verification
The individual signature of a node fails for message is invalid. Participants are disqualified if their individual signatures are found to be invalid. The remaining honest participants form the set and repeat the individual signature generation.

$$g^{si} = r_i^{H(M,R,h(y))} y_i^{L}{}_{\beta} \mod p$$

5.3Group Signature
A group signature is created after the update of all the nodes in the cluster with a individual signature by the cluster head. There by using this group signature a secure transmission path is established. These group signatures are added with the data when transmitted in the network.

5.4Threshold Signature Generation
After pj, j € α has received and verified t or more individual signatures the group signature on message m can be obtained as (R, S) computed as:

$$R = \Pi_{i \in \alpha} r_i \mod p$$
$$S = \Pi_{i \in \alpha} s_i \mod q$$

The function h(y) is attached to (R, S) and can be used later to trace the signers who collaborated to generate the threshold signature (R, S) on message m.
Threshold Signature Verification
To verify the validity of the group signature (R,S) for a message m by checking the following equation holds:

$$g^S = R^{H(m,R,h(y))} y_q \mod p$$

If equation holds, the group signature (R, s) for message m is valid.

6.PERFORMANCE ANALYSIS

MANETs have various security challenges compared to wired or cellular wireless networks. The Proposed work aims at establishing a secure data transmission communication channel using threshold signature scheme. Threshold multi signature scheme is based on a variant of the ElGamal signature scheme. A secure network is organized into clusters using one hop distance and elects the most qualified and trustworthy node as cluster head. A node has to gather information from its neighboring nodes to establish the trust for itself. Therefore the formation of Clusters based is done on the bases of the trust values among the nodes. It takes time for a node to collect enough data and to identify its neighboring nodes as malicious. From the experiment result about mobility, we found that most of the nodes stay in the same Cluster for few cycles until they reached the trust value of 1. Here an analysis is provided for system with respect to correctness, performance, and security. According to this experiment, our scheme is much lighter than previous threshold signature schemes. Moreover, this threshold scheme is comparable with

existing threshold signatures in non-ID-based cryptosystem.

7.CONCLUSION

Introducing clustering into the network topology reduces the communication overheads in MANETs. The Proposed work aims at establishing a secure data transmission communication channel using threshold signature scheme. Threshold-multi signature scheme is based on a variant of the ElGamal signature scheme. The selected clustering protocols for MANETs that describe various modifications carried over the node based Trust Management Scheme. The Cluster head selection algorithm is formulated by considering mobility of nodes. The nodes themselves determine whether they become Cluster heads using trust-value. As a trust model, performs better than confidant-extend in terms of packet successful delivery ratio and throughput. However, there are a couple of limitations in this approach. The way the messages passed through may overload the Cluster head, creating a bottleneck due to additional message exchanges. Another possible limitation is that the way that the message authentication between intermediate Cluster heads are treated, where there can be a delay in identifying a malicious neighboring node.

References

[1] Farooq Anjum , Dhanant Subhadrabandhu and Saswati Sarkar Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols Dept. of ESE UPenn Philadelphia PA 19104.

[2] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala Security in Wireless Sensor Networks: Issues and Challenges Universiti Technologi Malaysia Skudai, Malaysia IEEE 2013.

[3] Hero Modares Rosli Salleh Amirhossein Moravejosharieh Overview of Security Issues in Wireless Sensor Networks Department of Computer system and technology University of Malaya Kuala Lumpur, Malaysia IEEE 2011.

[4] Abhishek Jain, Kamal Kant M. R. Tripathy Security Solutions for Wireless Sensor Networks Department of Computer Science & Engineering ASET, Amity University Noida, India IEEE 2012.

[5] Bin Tian, Yang Xin Shoushan LU0, Xi ouYang Dong, Li Zhe Gong , Yixian Yang A Novel Key Management Method For Wireless Sensor Networks Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China IEEE 2010.

[6] Zheng Yue-Feng, Han Jia-Yu, Chen Zhuo-Ran, Li Zheng A novel based-node level Security strategy in wireless sensor network Computer Department of Jilin Normal University BoDa College of Jilin Normal University Si Ping ,China IEEE 2012.

[7] Adil Bashir, Ajaz Hussain Mir An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network Department of Electronics & Communication Engineering National Institute of Technology, Srinagar, Jammu & Kashmir, India IEEE 2013.

[8] Raihana Ferdous, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks

[9] Mehdi Maleknasab, Moazam Bidaki and Ali Harounabadi On TRUST Based clustering in Mobile Adhoc networks: Challenges and issues.

[10] Security Yan-Xiao, Xi'an, Qian-Liang Research On Wireless Sensor Network Telecommunication Engineering Institute Air Force Engineering University Xi'an, Shaanxi, China IEEE 2010

[11] T.Kavitha, S. Jenifa Subha Priya, Dr. D.Sridharan Design of Deterministic key pre distribution using number theory, Dept of Electronics & Communication Engg College of Engineering, Guindy, Anna University Chennai, India IEEE 2011.

[12] NGAI Cheuk Han Trust- and Clustering-based Authentication Service in MANET, Department of Computer Science & Engineering, Chinese University, Hongkong.

[13] Wenfang Wenfang Zhang, Xingyu, Xiaomin Wang A Novel ElGamal Type Threshold Signature Scheme without a Trusted Party Intelligent Control and Automation in Intelligent Control and Automation, Dalian IEEE 2006.

[14] Neeraj Kumar Mishra, Vikram Jain, Sandeep Sahu Survey on Recent Clustering Algorithms in Wireless Sensor Networks International Journal of Scientific and Research Publications 2013.

AUTHOR

Jeevan Yadav N S is working as a Lecturer in Computer Science and Engineering Department at Aakash International business Management College. He has obtained his Masters' degree from Jain University. He has graduated in Rajarajeshwari college of Engineering from VTU, Bangalore. He has presented and published 3 research papers in national and international conferences. He is also working as a department coordinator for Alumni Association and Workshops/Industry Visit.

Sindhu Anand received her M-tech. Degree in Computer science and engineering from Jain University, Karnataka, India in 2014. She has graduated in JSSATE College from VTU, Bangalore. Now she is a Research scholar in Jain University. Her experience and interest in wireless sensor networks and MANETs. She has presented and published 5 research Papers in international and National conferences.