Effective Trust Model for Public Key Management in Mobile Networks

S. Firthousia Parveen[*], Dr. M. Durairaj [**]

[*] M.Phil. Research Scholar, Dept. of Computer Science & Engineering, Bharathidasan University
[**] Assistant Professor, Dept. of Computer Science & Engineering, Bharatidasan University, Tiruchirappalli – 620 023

Abstract- Today mobile, wireless and non-static networks are getting more and more important as these are triggering the development of next generation networks to support mobile devices are bridging the border to traditional, static networks such as the internet. In public key storage management problem have arisen, because the key computation is still having high overhead and the potential threats of the key outflow or loss. In this research work, it is proposed a model approach of Effective Trust Model (ETM) to combine trust models and encrypt public key certificate which utilizes Ad Hoc on demand Trusted Distance vector (AOTDV) and are capable of operating without the support of any fixed infrastructure in Mobile Ad Hoc Networks (MANETs). Trust models essentially needed in order to establish reliable and high-performance communications. On-demand routing protocol is widely developed in ad hoc networks because of its effectiveness and efficiency. In this paper, the significance of Ad hoc On-Demand Trusted Distance Vector (AOTDV) routing protocol decreases the routing overload and end to end delay. This work concentrates implementation of identification and prevention of malicious nodes and message tampering attacks, using a semantic security mechanism.

Index Terms- Trust, public Key, MANETs.

I. Introduction of Trust Models

Employing public key based Effective Trust Models is predictable for the advanced security application in mobile ad hoc networks. In the security of mobile network architecture, the master seed key is securely stored in the universal subscriber identity (USIM) and generates the session keys such as the cipher key and the integrity key for mobile to use in the secure communication and application. Recent development of mobile communication technologies needed the deployment of the public key based security architecture for more advanced applications. While storing keys in USIM has the computational over head problem due to the security computations operated in USIM.

Therefore, our motivation is to overcome key management and key leakage problem. Since the communication is operated via wireless environment. Also, the mobile devices are always carried by users and can be lost. Moreover, their designs are related to the specific protocols such as AOTDV (Ad hoc On-demand Trusted Distance Vector) and sufficient to support the applications in mobile ad hoc network. The presence of wireless ad hoc networks all around us exacerbates privacy issues that must be addressed in order to prevent unauthorized observers. This work aims to improve the Trust Models resilient against not only the key exposure but also the key loss and to provide the secure and Effective trust models (ETM) for public key management in mobile networks. The trust model is based on MANET and achieves the great benefit regarding the efficiency of public key management.

This paper is organized as follows: Section 2 reviews related work. Section 3 discusses the key management and trust model in mobile ad hoc networks. A performance evaluation of the proposed approach is conducted in Section 4. In Section 5, conclude the paper and discuss possible future work.

1.1 Mobility-Based Key Management

The Mobility management is required in networks where the nodes are mobile. This is a particularly challenging issue in infrastructure networks. A mobile node that is communicating can leave the coverage area of an access point and enter another one. Establishment of trust in a MANET requires successful detection of intruders and isolating them promptly so that they may not exploit any network resources in the wireless network.

1.2 Trust Based Security Architecture for MANET

In general, trust is often described as the subjective belief of someone in the character, ability, strength, reliability, honesty or truth of someone or something. It provides tolerance to compromised nodes, have the ability to detect and remove adversaries from network and handle routing misbehaviors. The trust model defined in the architecture differs from related models by defending against both Flooding and Packet drop attacks

II. Related Work

E.Ngai [12] [2009] proposed another direction based on web of trust approach proposed in PGP, in which nodes act as CAs without any TTP. The system organizes the network into clusters, such that nodes are divided into different groups with unique identifiers. Nodes in the same group are assumed to know other, where each node monitors and keeps a trust table for storing trust values (defined as a continuous value 2 [0, 1] interval) for the behavior of its group members. Therefore, the protocol of certification between two nodes will be executed when both nodes belong to different groups.

Yi and Kravets [2004] provided a composite trust model. In their scheme they combine the central trust and the fully distributed trust models. This scheme takes advantage of the positive aspects of two different trust systems. Actually, it is a compromise between security and flexibility. Some

authentication metrics, such as confidence value, are introduced in order to glue two trust systems. However, proper assignment of confidence values is a challenge.

The main idea behind these approaches (Ngai.,2009) maintaining the trust table for each cluster nodes contain unique id. Yi and Kravets (2004) focus to avoid certificates altogether and bind the IP addresses of a node to its public key by deriving the former from the latter in a cryptographically verifiable way.

III. TRUST MODELS

3.1 Pretty Good Privacy (PGP) Trust Model

PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. PGP is a milestone in the history of cryptography, because for the first time it makes cryptography accessible to the wide mass of on-line public. It was principally created for encrypting or signing email messages. The PGP trust model created by Philip R.Zimmerman, 1991 [4] [1997]. Initially for the Internet in order to secure emails. PGP is based on referral certification, which allows multiple users to recommend a certain user by signing certificates of its public key. PGP adopts a system, called web of trust.

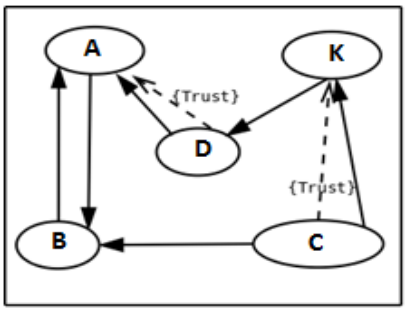


Figure 1 - PGP Trust Model

For example A signs B's public-key certificate which knows is authentic. B then forwards his signed certificate to C, who knows and trusts A as an introducer, finds out, after verification, that A is among B's certificate signer. Therefore, C can be confident that B's public key is authentic. However, had C not known or trusted any of B's signers, including A, she would have been skeptical about the authenticity of B's public-key. B would have to find another introducer whom C trusts to sign B's public-key certificate.

Trustworthiness of public-key certificate

- *Undefined*: We cannot say whether this public key is valid or not.
- *Marginal*: This public key may be valid be we cannot be too sure.
- *Complete*: We can be wholly confident that this public key is valid.

3.1.1 PGP Architecture

PGP breaks the traditional hierarchical trust architecture and adopts the 'web of trust' approach.

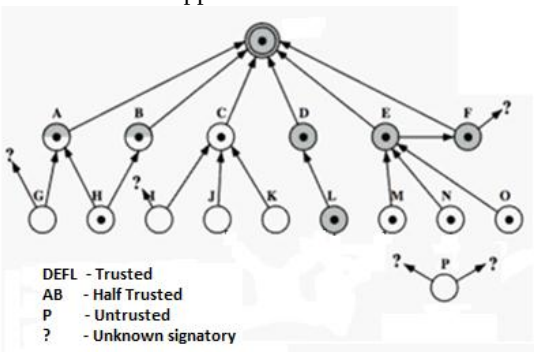


Figure 2 - PGP Trust model Architecture

There is no central authority which everybody trusts, but instead, individuals sign each other's keys and progressively forming a web of individual public keys interconnected by links formed by this signature. Public key certificates are central to PGP. Each certificate contains the key owner's user ID, commonly represented by the owner's email address in the form "name <userid@domain> the public key itself, a key ID of creation.

3.2 Distributed Trust Mode

Alfarez Abdul-Rahman and Stephen Hailes developed a distributed recommendation-based trust model [5] [1997]. The model's motivation comes from human society, where human beings get to know each other via direct interaction and through a grapevine of relationships. The same is true in distributed systems. In is the use of Threshold Cryptography in order to avoid the maintenance of a central Certification Authority (CA). The whole system has a public/private-key pair where the private-key is distributed over n of nodes. All nodes in the network know the public-key and trust any certificate signed by it.

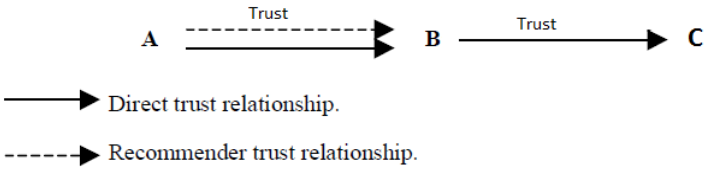


Figure 3 - Distributed trust model

3.2.1 Two types of trust Relationship

1. Direct Trust management

For every packet A sends to B, A puts a copy of it in a cache. If A sees B forwarding the packet correctly A promotes B for that. If A sees that B changed the packet or if A does not see the packet for some time, A punishes B. Then the packet is deleted from the cache.

2. Recommendation trust Management

The only option open to network agents for coping with uncertainty is via word of mouth, or recommendations. Trust, will always is hidden factors behind a decision to trust or distrust.

3.2.2 Trust Flow

For example, (the requestor) is requesting a recommendation from B(the recommender) about E (the target). A is interested in E's reputation for service, one of which A drives. A sends an RREQ to B because she trusts B as a recommender for car servicing mechanics, and B trusts C in a similar capacity. Since B cannot say anything about E with respect to "Car Service", B forwards A's RREQ to C, who may know. C in fact, knows about E's workmanship, and C believes that E's reputation for it is good, i.e. in C's opinion, E's trust value with respect to category "Car Service" is 3. C replies to B with are commendation in message 3. Notice that the Requestor ID and Request ID represents the last sender (or forwarder) of the RRQ in the forward RREQ chain.

A->B: A,rreqA01,E,[Car Service], T,20000101

B->C: B, rreqB01, E, [Car Service], T,20000101

C->B: B, rreqB01,[C],[(E, CarService,3,20000131)], PK_E

B->A: A, rreqA01, [C,B],[(E, Car Service,3,20000131)], PK_E

$tv_p(T) = tv(R1)/4 \times tv(R2)/4 \times .. \times tv(Rn)/4 \times rtv(T)$ (1)

$tv(T) = Average(tv1(T),..,tvp(T))$ (2)

3.3 Decentralized Trust Model

The decentralized trust model Introduced by Khare & Taylor, ICSE '04. The first decentralized trust-management systems, such as PolicyMaker [6]. The trust proposes an alternative solution. Basically, trust management uses a set of unified mechanisms for specifying both security policies and security credentials. The credentials are signed statements (certificates) about what principals (users) are allowed to do. Thus, even though they are commonly called certificates, they are fundamentally different from traditional name certificates. Usually the access rights are granted directly to the public keys of users, and therefore trust management systems are sometimes called key-oriented.

3.3.1 Architectural Approach for Decentralized Trust Management

The Practical Architectural Approach for Composing Egocentric Trust (Pace) provides detailed design guidance on where and how developers can incorporate trust models into decentralized applications. Pace's guiding principles promote countermeasures against threats to decentralized systems. Several prototypes demonstrate the approach's use and feasibility.

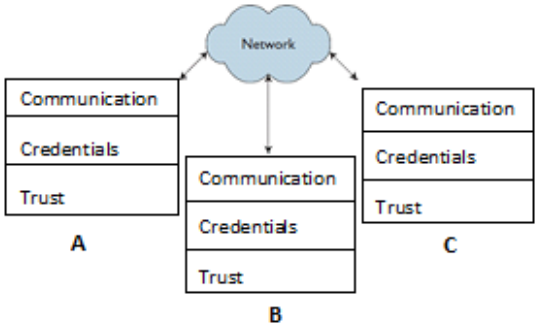


Figure 4 - Decentralized architecture

IV. ETM- The Proposed Approach

The term ETM refers the combination of Trust Models in wireless network. It is an approach to solve the problem of key distribution and management outflow and delay in signal. This can be achieved by mobile network based on wireless ad hoc network. Several mobile networks have adopted Java Network Simulation as their platform offered for developers. To certain extent Java applications are portable between devices. With this approach, the users can reduce significantly the outflow, attacks and delay in signal for sending message from source to destination. In this proposed work gives a formal description of a public key cryptosystem that includes the specification of trust model that combine PGP, Distributed and Decentralized model encrypt public key certificate for a secure environment. The AOTDV routing protocol decreases the routing overload and end to end delay. Confidentiality, integrity and availability are the key services and also the key assets that are protected.

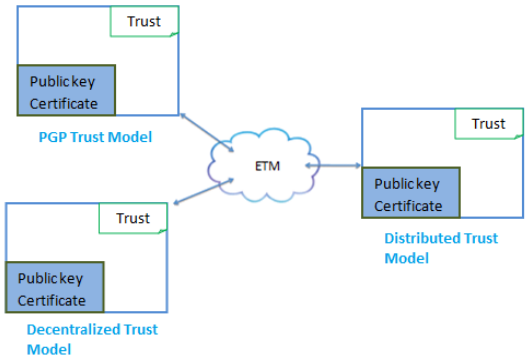


Figure 5 - Effective Trust Model

Cryptographic certificates are generated and held by the nodes of ad hoc networks, in order to prove their identities to nodes communicating with them, without the need of any central administration. These certificates are statistically unique and cryptographically verifiable, which means that it is very difficult that two entities hold the same certificate, and that it is possible to check the validity of a certificate by an entity.

Main Features

Every node carries a valid certificate and each server has its secret share stored in an encrypted format based on password. File transfer encrypted files through wireless network. The

trusted user and valid route reduce delay time and outflow and improve key management. The Security covers the protection attributes and the various challenges to security issues. The Reliable and security issues involve detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and preventing data packets.

4.1 Comparison

So far, the protocols have been analyzed theoretically [8] [2012]. Table 1 compares the result from these analyses and shows what properties the protocols have and do not have.

	AOTDV	AODV
Distributed	Yes	Yes
Energy Strength	Yes	No
Multicast	No	Yes
Loop Free	Yes	No
Security	Yes	No
Routing Traffic	No	Yes

Table 1 - Comparison between Ad hoc routing protocols

From the Table, all protocols are distributed and independent to easily configure in the event topology changes. The AOTDV support energy strength whenever the wireless node connected to server. And the route discovery prevent each time from the overlapping among the nodes. In AODV, loop free decreases hop count when intermediate nodes cross. They also added multicast capabilities to have route discovery mode to find new more routes. The main drawback in AODV carried source route in each packet. The security of AOTDV enhances high performance and communication.

Ad Hoc Wireless Mobile Networks
Mobile: topology changes dynamically
Ad-hoc: no designated infrastructure prior to deployment
Wireless Network: connectivity among nodes

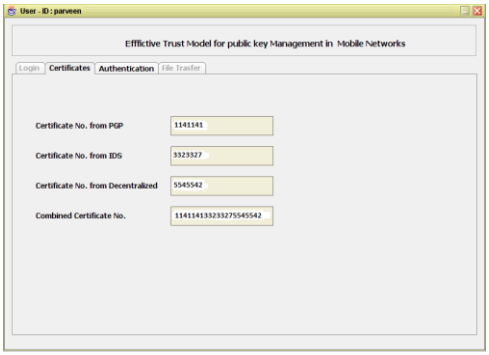
4.2 AOTDV Routing

In trust models, such as PGP, Distributed and decentralized models combine to provide a trust path and a node will collect all its neighbors' opinions about another node and combine them together using combination operations. The node transfer file from source to destination node. The security level and the trust levels of in between node cooperate to decide the encryption. The secure routing protocol based on Ad hoc On-demand Distance Vector (AODV) routing protocol. The new protocol, called AOTDV (Ad Hoc on demand Trust distance vector), has several salient features:

(1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them. (2) A node that performs malicious behaviors will eventually be detected and denied to the whole network. (3) System performance is improved by avoiding generating and verifying at every routing hop. The idea of the trust model can also be applied into other routing protocols of MANETs.

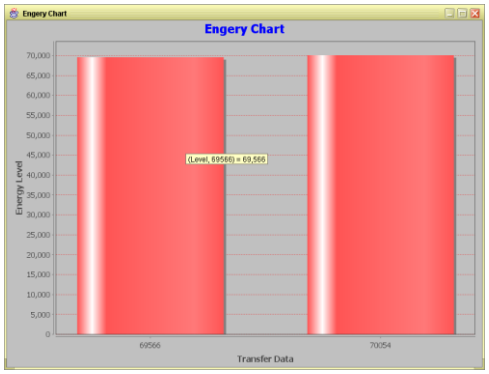
4.3 Experimental Analysis

The experimental results have been obtained from our proposed technique which is developed by using Java application and Net beans IDE 6.91. The implementation preferred to run on the windows 7 operating system. The Screenshot 1 shows the developed application for Effective Trust Models for Public Key Management in Mobile network. The ETM is achieved by combining the Trust Models to encrypt the message using RSA algorithm. The main objective of our simulation is to show that trust On-demand route establishment with AOTDV is highly secure and efficiency. Additional objective includes deducting outflow, overload and delay.



Screenshot 1 – Combination of trust model Credential

The AOTDV compute route discovery within secure routing solution which employs public key certificate authentication. Theses certificates are combined using ETM to establish the route. The encryption of file transfer from source to destination using AOTDV. The ad-hoc mobile network routing to the RSA algorithm that interface to the distance-vector router. The screenshot 2 shows the signal strength and trusted security of file transfer It is proved that AOTDV avoid the misbehaving links to protect clients.



Screenshot 2 – Signal Strength

V. CONCLUSION

This research, addresses the problem of absence of a central management in mobile networks and public key storage problem of the key outflow or loss. We propose a flexible Effective trust Models (ETM) based on the concept of human trust, which provides nodes with a mechanism to evaluate the trust level of its Neighbors. The basic idea consists of using previous experiences.

The combination of a trust models and public key encryption applies into the security solutions of MANETs. The trust and trust relationship among nodes can be represented, calculated and combined using AOTDV.. They can also perform trusted routing behaviors according to the trust relationship among them. Therefore, the computational overheads are reduced with the need of requesting and verifying certificates at every routing operation. The trusted AOTDV routing protocol is a more flexible security solution than other cryptography and authentication designs.

VI. Future Work

Future development can be made to enhance the AOTDV protocol, to further minimize load balancing to enhance the performance. Future work also includes the implementation of PKI Trust Models to compliment and optimize the efficiency of key management. The proposed model taken three models to security solution. Future work includes the integration of the all trusted models scheme with a secure ad hoc routing protocol to realize a complete security system.

References

[1] Bing Wu, Jie Wu, Eduardo B. Fernandez, Mohammad Ilyas and Spyros Magliverasb., "Secure and efficient key management in mobile ad hoc networks", Florida Atlantic University, Journal of Network and Computer Applications, 2005.

[2] Johann van der Merwe, Dawoud Dawoud and Stephen McDonald., "Trustworthy Key Management for Mobile Ad Hoc Networks", University of KwaZulu-Natal.

[3] Dagmara Spiewak and Thomas Engel., "Trusting the Trust-Model in mobile wireless ad-hoc network settings", Proceedings of the 5th international Conference on Information Security and Privacy, 2006.

[4] Alfarez Abdul-Rahman., "The PGP Trust Model", Department of Computer Science, University College London, 1997.

[5] A. Abdul-Rahman and S. Hailes., "A distributed trust model", Proceedings of the 1997 workshop on New security paradigms, 1997.

[6] Girish Suryanarayana, Mamadou H. Diallo, Justin R. Erenkrantz and Richard N. Taylor., "Architectural Support for Trust Models in Decentralized Applications", Institute for Software Research, University of California.

[7] K.Seshadri Ramana, Dr. A.A. Chari and Prof. N.Kasiviswanth., "Trust Based Security Routing in Mobile Adhoc Networks", K.Seshadri Ramana et al. / (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 02, 2010, 259-263.

[8] G. Rajkumar And Dr. K. Duraisamy., "A Review Of Ad Hoc On-Demand Distance Vector Routing Protocol For Mobile Ad Hoc Networks", Journal of Theoretical and Applied Information Technology, SASTRA University, Thanjavur, 2012. Vol. 36 No.1.

[9] Hakima Chaouchi and Maryline Laurent-Maknavicius., "Wireless and Mobile Network Security", ISTE Ltd John Wiley & Sons, Inc, 2009.

[10] William Stallings., "Cryptography And Network Security", Principles And Practice, Fifth Edition.

[11] Vikas Solomon Abel., "Survey of Attacks on Mobile Adhoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), University of Trinidad and Tobago, Trinidad.

[12] Mawloud Omar, Yacine Challal, And Abdelmadjid Bouabdallahfully., "Distributed Trust Model Based On Trust Graph For Mobile Ad Hoc Networks ", Computers & Security / Computers and Security 2009.

Authors

First Author – S. Firthousia Parveen, M.Phil. Research Scholar, Dept. of Computer Science & Engineering, Bharathidasan University, E-mail: sfparwin10.3@gmail.com
Second Author – Author name, qualifications, associated institute (if any) and email address. Dr. M. Durairaj, Assistant Professor, Dept. of Computer Science & Engineering, Bharatidasan University, Tiruchirappalli – 620 023, E-mail-durairaj.bdu@gmail.com