Security Server-Based Architecture for Mobile Ad hoc Networks

Salaheddin Darwish Simon J. E. Taylor Gheorghita Ghinea
Department of Information Systems and Computing
Brunel University
Uxbridge, UK, UB8 3PH
{ Salaheddin.darwish, Simon.taylor, George.ghinea}@brunel.ac.uk

***Abstract*— Mobile Ad hoc Network (MANET) is receiving a great attention by different communities (e.g. military and civil applications) thanks to its self-configuration and self-maintenance potentials. Securing MANET is a very critical matter as it is vulnerable to different attacks and also it is characterized with no clear line of defence. Since any security solution relies on a particular trust model, there are different types of trust models that could suit MANETs. This Paper present a design of security architecture based on the hybrid trust model. Our security architecture caters for improving services availability and utilisation.**

Keywords- Trust Models, PKI, Authentication, Threshold cryptography, Security Architecture

I. INTRODUCTION (HEADING 1)

Nowadays, Mobile Ad hoc Network (MANET) [1] [2] is receiving a great attention by different communities (e.g. military and civil applications) thanks to its self-configuration and self-maintenance potentials. It basically consists of a set of wireless mobile nodes enabled to communicate dynamically on the fly in multi-hop manner without any pre-existing network infrastructure (infrastructure- less). Unlike cellular networks and WLANs, every node participating in this network takes two roles simultaneously; it becomes a router to handle packets routing to other nodes and an application node (i.e. a user or service provider) to handle its own communications. Apart from that, each node is able to join and leave the network freely, and this renders its topology to change frequently [3] [4]. In fact MANET has a number of challenging properties. Its resources for example are stringent as majority of its nodes are_low-end devices normally powered by battery. On the other hand, MANET also exploits the current wireless technology (e.g. Wi-Fi, Bluetooth and IrDA) that already operate with limited bandwidth [5] [6].

Like any networking system, security of MANET is perceived from different points such as availability, confidentiality, integrity, non-repudiation, authentication, access control and usage control [6]. However, Securing MANET is a very critical matter. It is vulnerable to different attacks and also it is characterized with no clear line of defence. This is because of open wireless medium used and number of particular constraints in its properties: limitation in resources capability, intermission in communication and lack of physical protection. On the other side, variant in security requirements of MANET's applications is considered one of the challenges for deploying security solutions. For instance, depending upon the network purpose, its security requirements in the military settings vary according to the encountered circumstance. Confidentiality and availability are the most important issues in a battlefield, whereas in a humanitarian rescue mission scenario, availability is much more required than confidentiality. Therefore, the security requirements in every case stem from the tackled application context.

The trust is very important term which most security services (e.g. authentication, authorisation and etc.) rely on in their deployment. Therefore, in literature there are several trust models that their mission is to describe how to manage trust relationship between entities. Those models can be organised into two prominent approaches:

1- Models based on Third Trust Party (TTP), where TTP is a special entity (i.e. a fixed server) trusted by all the other entities. The credentials (certificates and/or keys) are issued by a single authority like PKI (public key Infrastructure) [7], or Kerberos [8] (or a group of special servers – collaboration between nodes to establish trust in the network – using for an example threshold cryptography [9]) .

2- Model based on Self-organisation or Peer-Trust, where security does not used any trusted authority or fixed server, the models based on trust propagation through a trust graph (PGP [10]). On the other side, schemes that are based on the reputation concept, where trust is amended according to the nodes behaviour are considered one of self-organised model for establishing trust.

This Paper preset a design of security architecture based on the hybrid trust model (i.e. combination of centralized and distributed models). It consists of a set of servers emulating certification authorities in order to manage certificates of joining nodes and help them in authentication.

The remainder of this paper is organized as follows. In section-II, we give an overview of related works. In section-

III, we present our propose security architecture for MANET. We end this paper with a general conclusion.

II. Related Work

This section reviews trust models in both wired networks and MANETs. Trust Model is categorized in three main classes: centralized models, partially distributed models, and entirely distributed or self-organized models.

A. Centralised Models

PKI (Public Key Infrastructure) is still acknowledged one of the most affective models for managing digital certificates (issuance, revocation and distribution) to trusted peers. Those certificates are essentially used for deploying security services, such as authentication, authorisation and digital signatures and encryption [7]. PKI relies on TTP (Third Trust Party) so-called CA (Certification Authority) the trusted entity in the system. In addition, PKI has been developed for wired networks and some infrastructure based wireless networks where there is no serious problem in connectivity and availability. It is noticeable in the PKI domain that security and scalability issues of CA are considered very crucial as CA is required to handle a large number of requests effectively.

Similar to PKI, Kerberos [8] developed by MIT is a centralized TTP-based trust model. The TTP is here referred to a KDC (Key Distribution Centre) which holds all shared secret keys for user and server principles. The role of Kerberos Service is to become the trust reference in the system. Kerberos shares different key-secrets with each entity in the network, and it creates session keys which are used among users and servers.

B. Partially Distributed Models

In [9] L. Zhou et al. proposed a partially distributed certification authority (CA) based on scheme of (k, n) of Threshold Cryptography (TC). The role of CA is distributed among specific nodes: servers, combiners, and a dealer. Servers and combiners perform signing public key certificates for users. The dealer is a particular server which holds the completely private-key certification authority. For any joining node, if all partial signatures are collected, it can then compute the complete signature locally to obtain the complete public key certificate. However, [11] Raghani et al. suggested a similar solution but this solution introduces an approach how to dynamically adjust the value of the threshold when required, and by this means decreases the certification delays.

In [8], S. Yi et al. adopted the TC–based scheme. They describe how to select particular nodes according to their best physical security and capability so as to be MOCA servers (MObile Certification Authority). Also communication overhead in this solution is apparently reduced by using the technique of caching routes to MOCA servers. The system utilises unicast instead of flooding when sufficient cached routes exist.

In [12] Luo et al. proposed DICTATE (Distributed CerTification Authority with probabilisTic frEshness for ad hoc networks). The DICTATE architecture presents a hierarchical CA between one mCA (mother CA) in wired network, and a group of dCAs (distributed CA) in MANETs. the group of dCAs relies on the TC scheme for signing a certificate of joining node. Nodes in MANETs can cooperatively be isolated from the mCA, but always have the need for CA's services. The mCA delegates a group of dCAs in order to increase the availability of security services when mCA is offline or out of reach.

In [13] B. Wu et al. proposed SEKM (Secure and Efficient Key Management in mobile ad-hoc networks). In SEKM, the CA trust is distributed to a group of nodes, which could be nodes with normal or better hardware in a mesh-based topology. SEKM the same as MOCA is designed to offer efficient share updating among servers and to quickly reply to certificate updating. For efficiency, only a subset of the server nodes initiates the share update phase in each round. A ticket based scheme is developed for efficient certificate updating.

In [14] Omar et al. devised a hybrid trust solution called NetTRUST (mixed NETworks Trust infrastRUcture baSed on Threshold cryptography). NetTRUST exploits two sets of a particular CA for managing PKI: central CAs (CCA) in wired network, and mobile CAs (MCA) in ad hoc network. MCA servers emulate the CA role by using a (k, n) scheme, and the CCA servers delegate the CA role to MCA servers by using a (t, m) scheme. The system leverages decentralisation, supports nodes mobility, and resists against MCA failures. Also this solution introduces the usage of the standard X509v3 certificate issued by CCA or MCA and demonstrates how to get benefits from the powerful attributes of X509v3 in this context, for more details in [14].

C. Entirely Distributed or self-organisation Models

PGP (Pretty Good Privacy) [10] is a completely distributed model which was created, by P. Zimmermann targeting Internet. PGP is developed to be a substitute to the conventional PKI based on trusted authorities in order to offer free practical security solution to protect low value communications, such as emails. The fundamental part of PGP is referral certification which enables multiple users to "recommend" a certain user (i.e. work as an introducer) by signing certificates of its public-key. PGP adopts a system, called "Web of Trust" which mainly facilitates and manages key distribution. However, this scheme has a drawback making it vulnerable because, for example, dishonest users may issue false certificates to cheat other users.

Based on the same idea of PGP, In [15], [16] Capkun et al proposed a self-organized trust model for MANETs, in which trust among nodes is maintained through physical contact. In this model every node issues public key

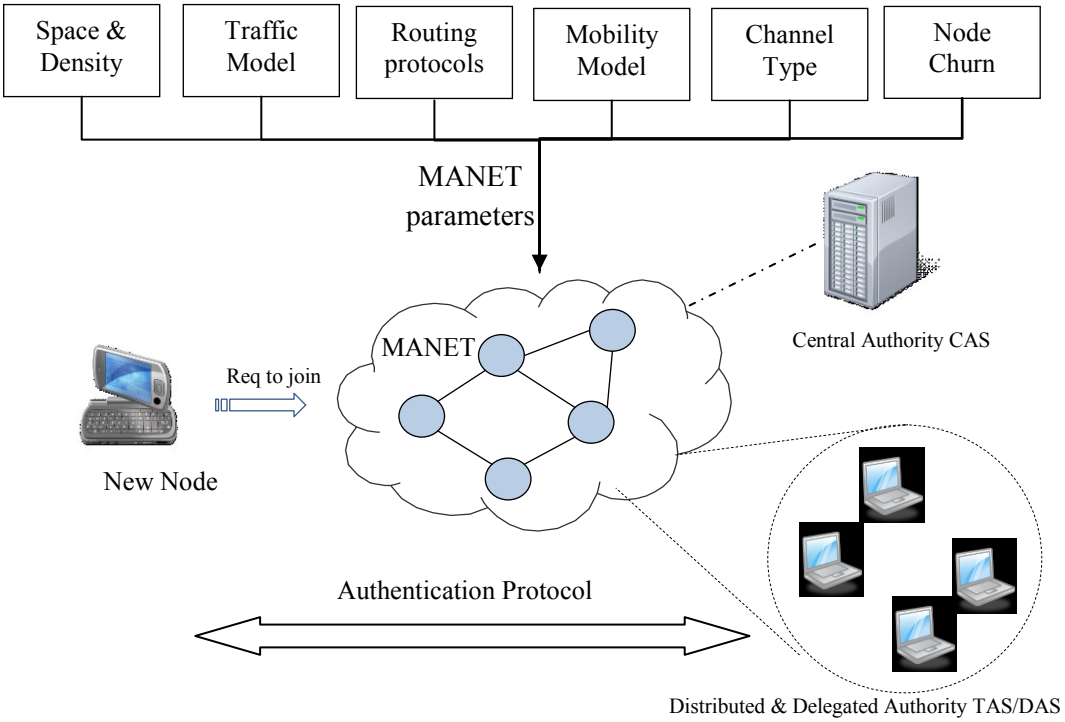

Fig. 1. Our proposed architecture

certificates to those who trust from its own domain. Nodes are able to authenticate each other with chains of trust regardless of the network partitions and without any centralized services. This model includes all required algorithms (e.g. the Shortcut Hunter algorithm) to facilitate the initialization and authentication process, and nodes are expected to store as many certificates as possible. In this model, trust is established from "offline trust relationships", which are created from general "social relationships".

In [17], H. Luo et al. proposed, for MANETs, a completely distributed certification authority model, based on threshold cryptography. The model distributes share among all nodes at the time when they join the network. When a new node wants to access to get its certificate, it sends a request to its k neighboring nodes for partial certificates. If the coalition decides that the requesting node is a "well-behaved node", they issue their partial certificates. These partial certificates are then combined together by the target node to create the complete certificate using an interpolation function. On the other hand, Trust is maintained by the notion that all the nodes must observe the direct neighbors behavior, and maintain their own CRL (Certificate Revocation List). In case, a node discovers one of its neighbors is dishonest, it adds its certificate to the list of revocations and disseminates through the network an accusation. If the certificate of accusatory is revoked, the accusation is ignored. Otherwise, the node is marked suspect by all the nodes receiving the accusation.

III. Our Proposed Security Architecture

In this section, we present our architecture and the framework how to evaluate it.

A. Motivation and Objectives

Our proposal is targeting a large scale MANET where there should be a hundreds of nodes joining the network in order to utilize offered and available services (e.g. video streaming, internet gateway etc.). On the other hand, we assume that MANET nodes are limited to mobile devices (smartphones or laptops) but there is a fixed server equipped with a wireless interface. We may consider this fixed server as an access point between the infrastructure-based network and MANET. The network can undergo disconnections and partitioning due to nodes mobility and churn (i.e. joining, staying, depleted, failure and leaving). The main aim is to define a trust infrastructure which fulfills the following properties:

- Maintaining higher availability and better scalability to security services.
- Improving the performance and efficiency of security services (an optimal round trip time or delay).
- Providing an appropriate level of protection through securing nodes and their communications.
- Adaptable to network partitioning and resources limitation.
- Offering flexible topologies of authorities. It means in regards every joining node has different

alternatives to be chosen in order to authenticate and obtain its certificate.

- Efficient certificate management (issuance, revocation, renewal).

B. Overview of Our Proposed Security Archicture

Our proposal is to come up with a novel security solution to handle trust and authentication in MANET efficiently and effectively covering different levels of operations (e.g. an application layer). This solution is practically describing how to make use of available different prioritized alternatives for trust models (e.g. centralized or distributed models) under particular settings of MANET. As shown in fig.1, those settings come from both MANET features and the scenario taking place, for examples, the type of network mobility, nodes churn and routing protocols etc. Our proposed security architecture consists of three main components as following:

1- Central authority Server (CAS): so-called the root authority is the highest trust entity. Despite the fact that the centralized trust model has a single point of failure; we adopted it for our solution as a vital part of a combined solution because we believe this model has good potentials to exploit in term of administration. On the other side, this central server is usually fully protected and well-equipped. CAS in initialization phase generates security keys and issues the required root and delegated certificates. Also it is responsible to elect Threshold authority Server and create and update their partial shares when it is necessary. Finally CAS performs authentication for the joining node by issue its certificate when it is reachable.

2- Threshold authority Server (TAS): this server has a partial part of private key own by CAS in order to use it in signing partial certificates. It normally creates and updates a partial certificate for the corresponding calling node. TAS is arguably available when CAS is offline. Node which has its certificate from this type of server must combine it with other partial TAS's certificates based on the (k,n) threshold cryptograph scheme. A subset of TASs actually represents the distributed trust model in this regard as shown in fig.1.

3- Delegated Authority Server (DAS). This server managing his own certificates. It creates certificates to the accessing nodes by using its own signature and attaches them with its CAS delegation certificates. Therefore a node which authenticates to this server gets the certificate chain in order to be able to validate and use to access to the available services within the network. Apart from that, we propose that TAS takes the task of DAS, in other words, one server node has two TAS and DAS services. This is because TAS server is already elected with high confidence by CAS. Which in turn reduces the overhead of performing election again and also TAS usually has a capability of running these two services.

On the other hand, the priority of trust models (i.e. server models) in this context is characterized and determined by two measurements, availability and a level of trust. We develop a priority list grading options of using the three types of servers: (1) CAS; (2) TAS; (3) DAS. The new node starts calling CAS first. In case CAS is not available, it moves to the second option of calling k TASs. If the calling k TASs fails to satisfy k answers, it picks one of reachable TAS to call the DAS service to get certificate chain. Every successful call of the option in this list is recognized with a distinguishable certificate which has a different level of trust as shown in fig. 2.

Eventually, the main purpose of our proposal is to maximise services utilisation, the more nodes have their certificates, in other words, they are authenticated, the more nodes are motived to get involved in operating MANET and exploit offered services. On the other side, using different levels of trust in the certificate would offer flexibility and security to the service providers. This is by enabling them to manage and control their service access according to these levels, for an example, a service provider sets a access policy to accept only the certificate issued by CAS from the calling node for safety reason.

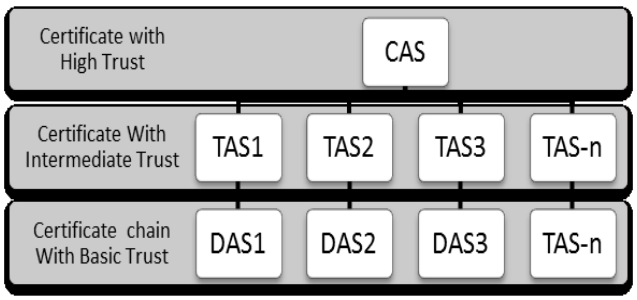

Fig. 2. The Trust Level of Certificate issued by different servers.

IV. *CONCLUSION & FUTURE WORK*

In this paper, our focus is on the trust models and infrastructures in both MANETs and wired networks. We present the three different categories: centralized models, partially distributed models, and completely distributed models. We then propose security architectures which provide a different subset of servers to work as certification authorities (e.g. CAS – Central Authority Server; TAS – Threshold Authority Server; DAS – Delegated Authority Server). These servers are to facilitate authentication to nodes in the network and issue node's certificate characterised with different level of trust. Our security architecture caters for improving services availability and utilisation. The next plan is to create an experiment approach to evaluate our architecture using a simulation. Simulation

study of this architecture is currently under way, using the network simulator OMENT++ [18] .

V. *REFERENCES*

[1] *IETF MANET group*. Available: http://datatracker.ietf.org/wg/manet/charter/

[2] *National Institute of Standards and Technology NIST, Wireless Ad Hoc Network , .* Available: http://w3.antd.nist.gov/wahn_mahn.shtml

[3] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*: Prentice Hall PTR, New Jersey 2004.

[4] C. K. K. Toh, *Ad Hoc Wireless Networks: Protocols and Systems*: Prentice Hall PTR, NJ, USA, 2001.

[5] I. Chlamtac, M. Conti, and J. J. N. Liu, Mobile ad hoc networking: imperatives and challenges, *Ad Hoc Networks,* vol. 1, pp. 13-64, 2003.

[6] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in mobile ad hoc networks: challenges and solutions, *Wireless Communications, IEEE,* vol. 11, pp. 38-47, 2004.

[7] R. Perlman, An overview of PKI trust models, *Network, IEEE,* vol. 13, pp. 38-43, 1999.

[8] B. C. Neuman and T. Ts'o, Kerberos: an authentication service for computer networks, *Communications Magazine, IEEE,* vol. 32, pp. 33-38, 1994.

[9] L. Zhou and Z. J. Haas, Securing ad hoc networks, *Network, IEEE,* vol. 13, pp. 24-30, 1999.

[10] A. Abdulrahman, The PGP Trust Model, *The Journal of Electronic Commerce,* 1997.

[11] S. Raghani, D. Toshniwal, and R. Joshi, Dynamic Support for Distributed Certification Authority in Mobile Ad Hoc Networks, in *Hybrid Information Technology, 2006. ICHIT '06. International Conference on*, 2006, pp. 424-432.

[12] J. Luo, J. P. Hubaux, and P. T. Eugster, DICTATE: DIstributed CerTification Authority with probabilisTic frEshness for ad hoc networks, *Dependable and Secure Computing, IEEE Transactions on,* vol. 2, pp. 311-323, 2005.

[13] B. Wu, J. Wu, E. B. Fernandez, M. Ilyas, and S. Magliveras, Secure and efficient key management in mobile ad hoc networks, *J. Netw. Comput. Appl.,* vol. 30, pp. 937-954, 2007.

[14] M. Omar, Y. Challal, and A. Bouabdallah, NetTRUST: mixed NETworks Trust infrastRUcture baSed on Threshold cryptography, in *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, 2007, pp. 2-10.

[15] S. Capkun, L. Buttyan, and J. P. Hubaux, Self-organized public-key management for mobile ad hoc networks, *Mobile Computing, IEEE Transactions on,* vol. 2, pp. 52-64, 2003.

[16] S. Capkun, L. Buttyan, and J.-P. Hubaux, Small worlds in security systems: an analysis of the PGP certificate graph, in *Proceedings of the 2002 workshop on New security paradigms*, Virginia Beach, Virginia, 2002, pp. 28-35.

[17] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, URSA: ubiquitous and robust access control for mobile ad hoc networks, *Networking, IEEE/ACM Transactions on,* vol. 12, pp. 1049-1063, 2004.

[18] OMENT++. Available: http://www.omnetpp.org/