Trust in Ad hoc Networks
A Novel Approach based on Clustering

J. Boodnah and E.M. Scharf

Department of Electronic Engineering, Queen Mary, University of London

Abstract

Ad hoc Networks by virtue of their nature pose a real challenge towards establishing trust among nodes within the network. This paper introduces and describes a novel approach, based on clustering, for establishing such trust. Studies on traffic generation in both the proposed method and a fully distributed approach show that the proposed method provides leaner trust establishment than the traditional peer-to-peer approach whilst not appreciably adding any further constraints to the network.

1. Introduction: Mobile Ad hoc Networks – Uses and Characteristics

Mobile ad hoc networks (MANETs) are designed for situations where no fixed or cellular infrastructure is available and where, indeed, decentralised network configurations are both advantageous and necessary. MANETs have therefore been considered for crucial military and civil applications such as battlefield scenarios and rescue operations in remote areas. Industrial and commercial applications include quick deployment of local coverage at construction sites and a means of providing wireless-based extended coverage for public access in urban areas. At the local level, ad hoc networks that link notebooks or palmtop computers could be used to share information at a conference or private meeting. On a more futuristic note, they might also be available for home networks where devices can communicate to exchange audio and video information, alarms and configuration updates.

Because there is no fixed infrastructure in an ad hoc network, the hosts themselves have to form it and it can therefore change at any time. All hosts capable of forming ad hoc networks are equipped with wireless transmitters and receivers.

Traditionally, because of the nature of ad hoc networks, research has mainly focused on routing issues. However, inherent with all the advantages an ad hoc network may offer is a vulnerability to security attacks that needs to be addressed.

2. Security and Trust – A Challenge for MANETs

Threats to ad hoc networks can be broadly categorised into: threats to the basic communication and routing mechanism, and threats to the security mechanisms such as key management mechanisms. There are various reasons why wireless ad hoc networks can be susceptible to security attacks, the principal ones being:

- ***Open Links*.** The wireless links between nodes are open and are hence very vulnerable to link attacks, which may include passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation, message replay, message distortion and denial of service.
- ***No Centralised Monitoring*.** MANETs do not have centralised monitoring and/or management points. Because of the lack of infrastructure, the usual practice of establishing a line of defence, distinguishing nodes as trusted and non-trusted is impeded. There are no grounds for an a priori classification. This makes it harder to monitor and manage the network.
- ***Dynamic Nature*.** The dynamic nature of the networks means that the network size can vary considerably and this means that the security architecture needs to be scalable to accommodate this possibility.
- ***Compromised Nodes and Routing*.** Mobile nodes can be physically captured and therefore compromised. Not being fixed devices, there is no scope for confining them up to secure rooms.

Attacks on communication and routing mechanisms need to be protected by the use of appropriate cryptographic techniques. For these techniques to work properly, the key management infrastructure must work first. This is simply because if a key management infrastructure is compromised, then a host cannot trust the key it obtains for cryptographic purposes, and if the key cannot be trusted, then encryption is worthless. Hence trust is a crucial and inherent pre-requisite for the security of ad hoc networks.

3. Trust as a tool for Security

Several approaches for building trust have been reported in recent work; these provide extensive definitions of trust as a concept. The novel Cluster Head (CH) approach, which is presented in this paper, draws on this work.

- **The Poblano Model** [1] presents trust relationships between peers and between peers and the data content, by using the risk factor and peer confidence (data relevance). It propagates trust via six degrees (Distrust to Complete Trust) and also has a recommendation system for security purposes.
- **Bayesian Networks** [2] have a theoretical foundation on Baye's rule. For instance, a root node T has two values (satisfying – 1, and unsatisfying – 0) and P(T=1) represents overall trust in an entity. This is measured as the percentage of satisfying interactions over the total number of interactions. An obvious disadvantage is that the selection of trust is too rigorous (0 and 1) while "satisfying" is a subjective and vague descriptor.
- **Semantic Web**. [3] This aim of this project is to build a "Web-of-Trust" that integrates trust and social networks and represents the concepts of direct and recommendation trust as a graph. It is implemented by extending of "Friend-Of-A-Friend" project and contains 9 levels of trust within a specific area (3 better than Poblano). Applications include Trustbot (IRC) and TrustMail (Mozilla).

These methods generally work on a meshed network model and can be seen as fully distributed networks (i.e. no clustering).

4. The Cluster Head Approach

The proposed approach uses a semi-meshed Public Key Infrastructure (PKI) model. Ad hoc networks, due to their randomness can be compared to meshed networks but it is important to note that security requirements can vary quite dramatically depending on the scenario in which they are applied. For instance, military scenarios will have more stringent requirements in trust establishment than say a LAN-based party game, or even participants at a conference. In our case, a conference scenario is adopted with the following *assumptions*:

- **A Priori Trust Information.** Some nodes in the network have some a priori information about one another and therefore have some form of trust relation albeit in varying degrees. This evidence may have been obtained off-line (as in visual identification), by an audio exchange, or even physical contact. Such an assumption is not unrealistic since most ad hoc network scenarios will generally have some nodes that can be paired with others in terms of trust relationships.
- **Reachability.** Each node is within range of any other in the whole network and all nodes are interconnected at the start of the simulation.
- **Computational Resources.** Each node has sufficient computational power to be able execute any required encryption algorithm and be able to generate or sign certificates. Each node has sufficient memory for public key storage.

4.1 PKI and Trust

PKI makes use of a public key which is used to encrypt the message and a private key which is used to decrypt it. Trust issues arise when nodes have to authenticate one another in order to be able to send encrypted information over the air interface. In order to use a key, a node has to be absolutely certain that the public key effectively belongs to the recipient node. This is normally achieved via the use of certificates. In ad hoc networks, certificates are issued by the nodes themselves. This means that nodes have to be able to trust each other and hence generate those certificates. Trust values are an ideal way of achieving this.

A trust value can be a denomination that has been achieved by a recommendation or via an existing trust relationship. Basically, trust value is very similar to reputation except that they are, in this approach, between two single nodes only (i.e. the cluster head and the member node). A reputation is mathematically the mean of all recommendations. It can also be defined as an import of the past behaviour of a node.

4.2 Network Topology and the Role of the Cluster Head

The strategy used in the proposed model is to implement mini hierarchal structures in an otherwise meshed PKI model. The idea is to use a cluster-based network, for the purpose of establishing trust only noting that clustering was originally used to minimise the flooding of route discovery packets [4]. In our system, the entire network is divided into a number of clusters as shown in Figure 1. A cluster has a cluster head (CH) with the following attributes.

- A cluster head (CH) is elected for each cluster to maintain the cluster membership information.
- Each cluster is identified by its Cluster Head ID and each node in the network knows its cluster head and therefore knows which cluster it belongs to.
- A node belongs in a cluster when it has a duplex link to the head of that cluster. For discussion purposes we refer to it as a slave node.

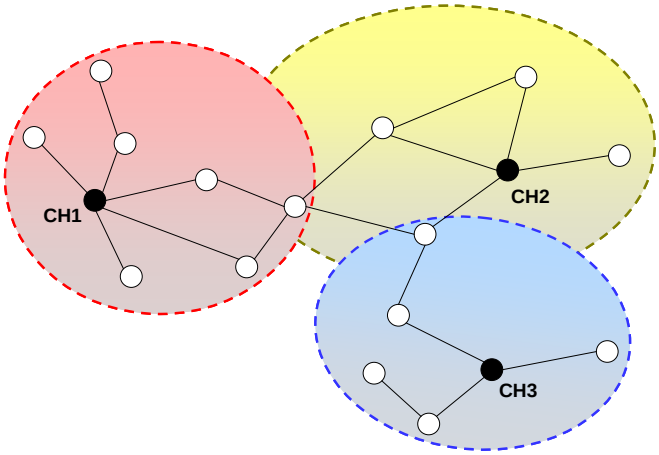

Figure 1: The Cluster Head Approach to Trust Establishment

For distributing trust within an ad hoc network, the following aspects are also introduced.

- The CH is elected on a democratic basis. This means that the node with the most trust relations with other nodes in its surroundings is assigned the role of CH. Should a CH leave a cluster, the next available node down the trust hierarchy is chosen.
- This means, that for simulation purposes, once a cluster is formed, all slave nodes trust the CH and therefore all nodes with the cluster trust one another other (via the CH which is responsible for propagating trust certificates).
- Within the cluster, the PKI follows a hierarchal model. This is because it is assumed that all nodes within a cluster will trust the CH who will then act as a mini Certificate Authority (CA) for that cluster. A meshed model is however in place for inter-cluster trust relationships.

5. Simulations

Initial simulations are carried out in NS-2. The conference scenario is modelled as a collection of six clusters each with six individual nodes, excluding the cluster head, hence providing 42 nodes in total. The CH method is compared to how it would fare in a fully distributed network (with all network nodes being considered equal).

Trust is propagated within the network via the use of trust certificates with a set size of 1024 bytes. This conforms to realistic estimates of certificate sizes. Certificates include the node ID and associate that node ID with a public key. For simplicity the public key is limited to 6 characters. Number of nodes is 42, with a total simulation time varying from 30 to 90 seconds. Certificate requests are sent at the rate of 1 per node per link with zero delay and the whole scenario is implemented using UDP agents and constant size trust packets.

The simulations were run in the following order:

- Certificate exchange with cluster head inside cluster (increasing cluster size gradually).
- Certificate exchange between clusters (increasing number of clusters).

In this experiment, the main aim was solely to establish the total traffic, therefore an indication the total bandwidth consumed by the trust mechanism on its own. The system was not brought into any form of congestion to prevent dropped packets and the duplex links were set at an above-threshold bandwidth. Nevertheless, the system was brought to the worst case scenario in each incidence (to determine the maximum possible bandwidth consumption). These included:

- Simultaneous sending of key certificates from individual nodes to their CHs.
- All nodes request certificates from one another (in the fully distributed mode). This is extreme because it would be highly unlikely that this should happen in real life. However, it provides a useful upper bound for the bandwidth consumption.
- The system is considered trustworthy, when all nodes within the cluster or network have access to the certificate of every other node within that cluster/network, whether via the CH or individually.

The following outcomes were noted as are detailed in Figure 2 (a) – (d):

- In (a), it can be clearly inferred that the CH approach generates less overall traffic *within* the cluster. This advantage increases as the number of nodes increases. However, this can only go up to the congestion limit of the CH, that is the maximum number of certificate requests it can accommodate without starting to drop packets.

- In (b), the same experiment is repeated as in (a) but this time increasing numbers of clusters with fixed sizes (6 slave nodes) are compared in both cases. Again, the CH approach generates less traffic and this time, the larger the network, the better the CH approach fares.
- Figure 2(c) compares the amount of traffic within a cluster at the CH and the slave node (for the CH approach) and at each node (for the distributed traffic). This indicates that the while the CH has to accommodate more traffic than its slave counterpart, that traffic is no more than what any node would have to accommodate in a fully distributed scenario. Hence the CH method allows the slave nodes to have more resources for other purposes, unrelated to trust propagation.
- Finally, as a statistical confirmation, the average traffic per node is calculated for each method, confirming the superiority of the CH approach.

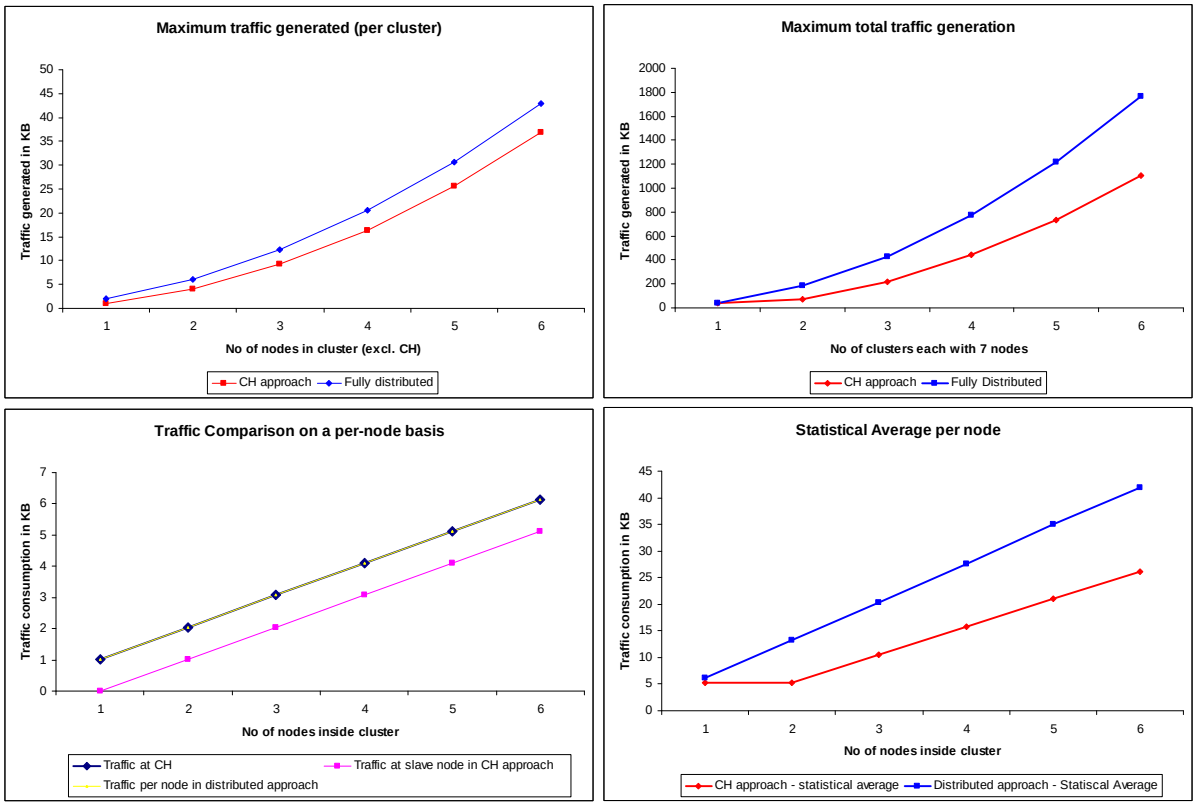

Figure 2 – Simulation results - clockwise from top left – (a), (b), (d), (c)

6. Conclusions and Future Work

The CH model presents several advantages over the fully distributed approach with regards to trust establishment. Because of the use of hierarchal PKI within the cluster, much less bandwidth is needed to establish trust between nodes within a cluster. However, such a method also has some drawbacks such as restricted a restricted cluster size. The initial trust establishment process is also assumed to be a priori and not generated. While these initial simulations are favourable with respect to the CH approach, other aspects of this particular method will be considered in future work. Some of those include the speed at which the network establishes trust, using mobile nodes with different routing protocols and varying the certificates' (hence packets') sizes, monitoring the trust mechanism close to congestion point and using varying trust values within and between the clusters. A trust maintenance model is also targeted whereby it will be possible to enable dynamic formation of trust clusters (that operate on top of the normal routing infrastructure) and implement trust distribution graphs.

References

[1] Rita Chen and William Yeager, "Poblano, A Distributed Trust Model for Peer-to-Peer Networks," http://www.jxta.org, Sun Microsystems.

[2] Yao Wang, Julita Vassileva: Bayesian Network-Based Trust Model. Web Intelligence 2003, pp 372-378.

[3] http://trust.mindswap.org

[4] Mingliang Jiang, Jinyang Li, Y.C. Tay, "Cluster Based Routing Protocol" August 1999 IETF.

Table of Contents – for Reviewers

Presentation Medium

MS PowerPoint (Office version 2000)

Authors' Details

1. Javesh BOODNAH
Department of Electronic Engineering
Queen Mary, University of London
Mile End Road
London E1 4NS
Tel: 020 7882 7408
Fax: 020 7882 7997
Email: javesh.boodnah@elec.qmul.ac.uk

2. Dr. Eric M. Scharf
Department of Electronic Engineering
Queen Mary, University of London
Mile End Road
London E1 4NS
Tel: 020 7882 5343
Fax: 020 7882 7997
Email: e.m.scharf@elec.qmul.ac.uk