Journal of Computer and System Sciences 77 (2011) 677–686

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Network trust management in emergency situations

Arjan Durresi [a,*], Mimoza Durresi [a], Leonard Barolli [b]

[a] *Department of Computer and Information Science, Indiana University – Purdue University Indianapolis, Indianapolis, IN, USA*
[b] *Fukuoka Institute of Technology, Fukuoka 811-0295, Japan*

ARTICLE INFO

Article history:
Received 15 September 2009
Received in revised form 5 January 2010
Available online 25 February 2010

Keywords:
Trust managements
Ad hoc networks
Emergency networks

ABSTRACT

We study the unique trust management, and more precisely reputation management and revocation of malicious nodes in the context of ad hoc networks used for emergency communications.

Unlike in centralized systems, reputation management and revocation in ad hoc networks is non-trivial. This difficulty is due to the fact that the nodes have to collaboratively calculate the reputation value of a particular node and then revoke the node if the reputation value goes below a threshold. A major challenge in this scheme is to prevent a malicious node from discrediting other genuine nodes. The decision to revoke a node has to be communicated to all the nodes of the network. In traditional ad hoc networks the overhead of broadcasting the message throughout the network may be very high. We solve the problem of reputation management and node revocation in ad hoc networks of cell phones by using a threshold cryptography based scheme. Each node of the network would have a set of anonymous referees, which would store the reputation information of the node and issue reputation certificates to the node with timestamps. The misbehavior of a particular cell phone is reported to its anonymous referees, who issue certificates which reflect the positive and negative recommendations.

1. Introduction

While we have developed a very rich communication environment, including a very reliable telephone network, wired and wireless Internet, cell phones and WLANs, all of them fail when the respective infrastructure is damaged, such as in natural or man made disaster situations. We believe that the research community should develop technical solutions to guarantee necessary and vital communications in future emergency situations.

Cellular phones are ubiquitous. They offer many more features than traditional phones and connect to the network using RF communication. It is estimated that there are about 271 million mobile phone users in USA [1], covering 88.04% of population. Cell phones have a low power transceiver which communicates with the base stations that are typically located a distance of a few miles. The base station connects the cell phone to the backbone telephone network. The cell phones cannot communicate when they are unable to connect to the base station [2].

There are many applications that would greatly benefit from using cell phones in ad hoc mode. During natural disasters, such as hurricanes and earthquakes, the cellular phone and the traditional phone infrastructure are usually damaged. Enabling cell phones to communicate in the ad hoc mode provides mechanisms for people trapped in buildings or elevators to seek help. These networks can also help the agencies plan and coordinate the relief effort. The communication architecture that we assume for emergency situations, is illustrated in Fig. 1. We assume that cell phones, besides their normal cellu-

[*] Corresponding author.
E-mail addresses: durresi@cs.iupui.edu (A. Durresi), mdurresi@cs.iupui.edu (M. Durresi), barolli@fit.ac.jp (L. Barolli).

0022-0000/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcss.2010.02.008

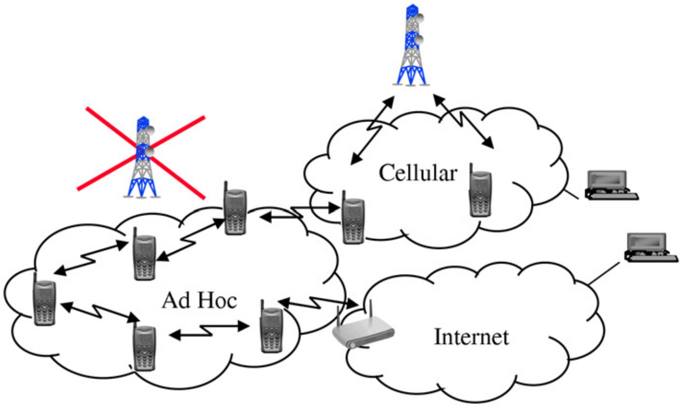

Fig. 1. Ad hoc network of cell phones. Initially, the base stations are alive and all cell phones are connected to the base station. When the base stations stop working, the effected cell phones communicate in ad hoc mode.

lar interface, are equipped with physical interface such as the 802.11 family to communicate among themselves in ad hoc mode, when their infrastructure is no longer available. We also assume that, in emergency conditions, broadcast will be the most needed model of communication. In addition, we also assume that cell phones can connect to the base station during normal mode, and the ad hoc network during emergency mode, as shown in Fig. 1. The ability to switch from centralized mode to ad hoc mode will allow cell phones to leverage the advantages of both systems.

The application of cell phones in ad hoc mode in emergency conditions requires data to be transmitted to all users. Therefore, we consider that data confidentiality is not a requirement. The ease with which a user can communicate with a large number of other users makes this system vulnerable to attacks ranging from pranks to terrorist attacks. Terrorists could artificially increase the population of an area by asking all other cell phone users to go there before a terrorist attack. To ensure that the perpetrator of these attacks is identified, the proposed solution offers secure broadcast authentication and guarantees non-repudiation. This approach is reactive because it identifies the attacker after the attack. Clearly this is not enough to stop all attacks that are possible with this system. Protocols need to be developed which would prevent a malicious cell phone user from misguiding other users [3].

In this paper we present a scheme for reputation management and node revocation in a distributed ad hoc network of cell phones. Each phone would have a reputation, score which is uniquely mapped to its ID. From here on we refer to the cell phone as node and the reputation score as score. When a node believes that another node is malicious it attempts to reduce the score of the node perceived to be misbehaving. When the score of a node becomes less than a predefined threshold, the node would then be revoked. This scheme also takes into account the fact that a malicious node may attempt to revoke a honest node.

When the nodes are connected to the base station, they can obtain the necessary key information which is used to communicate securely in the ad hoc mode. The base station assigns keys and ID's for the nodes in the ad hoc mode. The ID's in the ad hoc mode are not related to the ID's in the normal mode to ensure anonymity. For each node, there are n other nodes which are given a share of the key required to sign the score certificate. Out of the node certifiers k need to agree on a new score and sign a new certificate. When the network moves into the distributed mode from the centralized mode, each node has to obtain certificates of score from its anonymous certifiers at regular intervals. Whenever a receiver of a broadcast message believes that the sender is malicious, a message is sent to the anonymous certifiers of the node. The certifiers remain anonymous because nodes communicate with them in the ad hoc mode without any knowledge of their real identities. When the number of these messages becomes large, the anonymous certifiers give the node a new score certificate. There may be special nodes in the network which have more than one share of the group key. These trusted nodes may be important people like cops, mayors, etc. who we believe can be trusted. The number of shares of the key given to each of those trusted nodes is a design parameter. We believe that the efficient use of these trusted nodes would give us the same level of security with less overhead.

Reputation is defined as the perception that a node creates through past actions about its intentions and norms [4]. The reputation of a node is based on the perception regarding its behavior held by other agents based on its experiences and observations of its past actions [5]. Such experiences are conveyed through recommendations which can be both positive and negative. The major challenge for reputation based systems is assessing the truthfulness of such recommendations. In ad hoc networks, the absence of a commonly trusted entity means that the reputation system has to be distributed to the nodes of the ad hoc network. When the system is distributed, there may be an issue of recommendations that may contradict each other. The reputation systems in ad hoc networks need to be robust against contradicting reputations [6].

The three main attacks against a reputation based systems are the free rider problem, defamation and collusion [5]. In the free rider problem nodes do not share the reputation information with their peers. If a significant number of nodes do not communicate about the misbehavior of malicious nodes, then the nodes of the network will not be able to identify the malicious nodes. We believe that this problem can be solved by rewarding people for sending information about malicious nodes. Although this is an important problem, its solution is out of the scope of this paper. The second attack on a reputation based system is defamation. In this attack a malicious node attempts to defame a honest node and tries to get it revoked. Our scheme handles this problem by increasing the number of nodes which believe that a particular node is malicious. Even if a malicious node is part of the anonymous certifiers, it cannot sign a revocation certificate without $(k-1)$ other nodes. The third common attack on reputation based systems is collusion. Here a node tries to improve the score of another node by sending multiple positive feedbacks. Our scheme avoids this problem because scores are not increased in the ad hoc mode. They are increased once the nodes go back to the centralized mode. The central base station would be able to track multiple recommendations from the same node and prevent collusion.

This paper provides a mechanism to adjust the reputation score of a node in the ad hoc mode using threshold cryptography. The scheme also allows a group of anonymous certifiers to revoke a node based on the recommendations of other nodes. These recommendations are also subjected to scrutiny and there may be recommendations which provide feedback on the quality of recommendations. This would ensure that nodes which broadcast malicious recommendations are also revoked. The recommendation messages are designed in such a way that the recommenders and the recommended can be identified unambiguously. All the information can be collected once the base station is back online. The base station can then determine the malicious nodes. We would like to mention that the recommendations made by the users of the network are based on their own experiences which may not be similar to the experiences of other nodes. This paper does not deal with the aspect of decision making in these networks. There are many factors which may influence decision making which are out of the scope of this paper.

The structure of the paper is as follows. Section 2 presents some related work in the area of trust and cryptography. In Section 3 we discuss the system model for which we propose our scheme. Section 4 describes our scheme in detail. Section 5 presents the analytical and simulation evaluation of our solution, and we conclude in Section 6.

2. Related work

We have proposed a protocol which can be used to establish non-refutable communication for cellular phones in the ad hoc mode [7]. Unlike those of other ad hoc networks, the nodes of these networks are part of the centralized network before they enter the ad hoc mode. This allows these base station to send all the key information securely using the secure cellular infrastructure. We achieve secure non-repudiation in these networks by the use of Identity based cryptography. Details on the implementation of this scheme are presented in the next section.

Security on Cellular Networks is discussed in [8]. In [9] are presented various ways to use cellular network in emergency situations.

In [10] is presented one of the earlier works on trust. Reputation management has attracted much attention in ad hoc network too [11–13]. Uncertainty is examined to refine reputation computation in [14–18]. The effect of distrust propagation is discussed in [19]. A good review of trust management in mobile ad hoc networks is presented in [20] and of trust for online services in [21]. We have presented a solution for trust management in emergency networks in [22].

Kinateder and Rothermel describe two usage scenarios for a reputation based system, namely publishing recommendations and requesting recommendations [23]. In a publication based system, an entity which interacts with the target and decides to create a recommendation, publishes (broadcasts) the recommendation to all nodes of the network. On the other hand a requesting recommendation scenario is one where the entity which has to interact with the target enquires about the reputation of the target. In this paper, we present another usage scenario where, the node in question stores its own reputation value which is signed by the anonymous certifiers.

Many of the desired properties in a reputation based scheme for mobile ad hoc networks have been listed in [5]. The system should be able to unambiguously distinguish between the malicious and non-malicious nodes without the use of any centralized infrastructure. The system should also be robust to common attacks like node inactivity, defamation and collusion by a small number of nodes. Another important requirement is the timeliness of the information provided. The system would not useful if the malicious nodes are detected long after all the damage is done. Our scheme provides a trade-off between the communication overhead and the timeliness of reputation information.

The lack of infrastructure in the ad hoc mode means that the schemes for trust establishment can only depend on the local interaction of the nodes. In this situation trust management should start with a small group of trusted nodes which gradually establishes trust with the initially neutral members of the network. The whole network evolves from trust islands into a trust graph [24]. In the context of cell phones in the ad hoc mode, a broadcast would be trusted if the node can obtain a certificate from one of the few trusted nodes in the network (like cops/mayor etc.). If the node leaves the neighborhood of the trusted nodes, then their broadcasts have no trust. This approach may not be scalable if the number of nodes is much greater than the number of trusted nodes. Moreover, mobility of various nodes would also cause problems with location dependent security.

Ref. [25] utilizes threshold cryptography for the distribution of trust in the ad hoc mode. In this scheme signing key of the CA can be split into n pieces such that each node gets a piece of the information. Any k of these n can be used to recreate the private key of the CA. Even if $(k-1)$ malicious nodes collaborate, they would not be able to generate the key information. The disadvantage of this scheme is that if the number of adversaries becomes more than k the security of the entire network is compromised. In our scheme, security decreases much more gracefully with the increase in the number of attackers.

Ref. [26] presents a scheme which assumes that all nodes are connected to each other all the time. They all maintain a profile table which has the accusations against all the nodes of the network. The weights of the accusations of all nodes are different. The weight of the accusation of a node depends on the number of accusations against itself. This paper assumes that the all the nodes of the network would have exactly identical profile tables and those which have a different profile table are malicious.

3. System model

The nodes of the network are cell phones. They have significant battery power, computational power, communication range and memory. This makes them suitable for the use of asymmetric key cryptography. Our scheme is useful only when the cellular phone infrastructure is dysfunctional. Reputation Management and node revocation are trivial in a centralized system because all nodes can communicate only through the base station. We assume that the number of base stations that would be impaired at any point in time would be small. This combined with the fact that the communication range of nodes is large, means that a node can send data to the entire network in few hops. We also assume that the density of nodes in the deployment region is large. It is also assumed that more than k of the n anonymous certifiers for each node would be honest. The values of k and n are calculated after analyzing the tradeoff between security and overhead.

The base station of the cellular network distributes all the key information which would be used by the nodes when they are unable to connect to the base station. The base station creates an ID for each node which cannot be derived from the ID of the phone. We believe that Identity based Cryptography (ID-PKC) [27,28] would be best suited to this scheme. The base station generates a private key corresponding to each ID using some private information. The private key of each node is securely transmitted to the node using the cellular infrastructure. ID-PKC avoids the overhead for the verification of certificates because the public keys are generated using the ID's. If each node has to generate a new public/private key pair and get the public key signed by the *CA* (base station), the overhead is high. Instead if the base station generates the $\langle ID, PrivateKey\rangle$ for each phone and sends this pair to the phone using the secured cellular infrastructure, the overhead is considerably less. This scheme also takes the burden of key generation from the cell phone and gives it to the base station. The private keys corresponding to an ID are generated using a Private Key Generator (PKG) of the cellular network. Any node with the public key of the PKG can derive the public key of a node using its ID.

An ad hoc network of cell phones has more vulnerabilities than other instances of the mobile ad hoc networks because node capture is trivial. One cannot prevent attackers from being parts of the network because cell phones are freely available in the market for purchase. Any security scheme proposed for this environment must be able to address this problem. In this paper we assume that the number of malicious nodes in the network is very small compared to the total nodes of the network.

Based on the maximum number of malicious nodes expected, the tradeoff for the level of score when a node is revoked are decided. We define the reputation score from 0 to 1, where 0 signifies no trust and 1 signifies maximum trust. The initial score for each node is assigned by the base station. This score may be based on many factors like criminal history, credit history etc. which are out of the scope of this paper.

The honest user of the network is the most important part of the detection of the malicious nodes. Whenever the cell phone of a user receives a message, the user of the cell phone analyzes the message and performs the appropriate actions for his safety. But, when a user believes that the message was incorrect (or malicious) he sends a negative recommendation to all the anonymous certifiers of the sender. Free rider problem is a major problem in reputation based systems. This deals with the willingness of the attacker to report the malicious behavior of a node. In this paper we assume that a honest node would report the malicious behavior of a node because of the horrific consequences which may be caused if the user does not respond. We believe that a combination of laws with punishments for withholding information and reward for honest participation may also help. This aspect of the protocol is for the law enforcement agencies to address and we believe that it is out of the scope of this paper [29].

There may also be an incentive based approach where the honest user gets some benefits for reporting the malicious users.

4. Our scheme

In emergency situations when the base stations of the cellular network become dysfunctional, the nodes collaborate and form an ad hoc network. These networks can be used by users to communicate information and coordinate relief effort. This application is very powerful because a user can communicate with all the other users of the network. To detect the misuse and abuse of this system, a strong implementation of non-repudiation is required. All the messages sent during the ad hoc phase can be analyzed once the network returns to the centralized mode i.e. base stations start functioning. The main drawback of this approach is that the malicious nodes are detected only after the attack. This is clearly not enough defence against attacks which are meant to cause massive destruction and loss of lives. To prevent these attacks from occurring, a mechanism is needed to revoke the malicious nodes as soon as they are detected. We solve this problem using a reputation based scheme where the malicious nodes are detected and revoked.

We have developed a protocol for key distribution in an ad hoc network of cellular phones [7]. Our protocol utilizes the property in cellular phones where information required during the ad hoc mode can be securely distributed to the nodes using the infrastructure of the cellular network. Once the nodes go into the ad hoc mode they use this information to communicate with other nodes. We build this reputation based system on top of our existing protocol for non-repudiation which uses identity based cryptography.

The protocol assumes that each node has a private key corresponding to its ID in the ad hoc mode. We want to emphasize here that the ID of a node in the ad hoc mode is not same as its ID in the cellular mode. This is done to ensure anonymity in the ad hoc mode. This also prevents adversaries from mounting attacks against specific nodes of the network. If a node broadcasts messages using a known identity, the node's location privacy may be compromised. These problems are resolved when we use separate ID's for each node. These ID's are assigned by the base station and only the base station is able to derive the real ID of a node from the ad hoc ID.

The protocol starts with the base station assigning each node an ID, private key corresponding to the ID. Messages signed using the public key can be verified using the ID. The IDs are divided into groups such that each group has an ID which is the function of the IDs of all the nodes in the group. The private key corresponding to the group ID is split into *n* shares of which any *k* shares could reconstruct the group key successfully. For each node all the members in its group are its anonymous certifiers. Each node is given its reputation score in the form of a certificate which has the its ID and score. The certificate is signed by the private key of its group. Anyone with the ID of the node (from which the ID of the group can be derived) can verify the score of a node.

After the nodes enter the ad hoc mode, the broadcast messages to the entire network. Whenever the receiver of a broadcast message believes that the sender of the message is malicious, the receiver sends a negative recommendation to all the autonomous certifiers. When the current certificate of the sender expires, it would need a new certificate from the anonymous certifiers. The new certificate would reflect the negative recommendations for the node and reduce the reputation score of the node. If the reputation score of a node goes below a certain threshold, the anonymous certifiers revoke the node by broadcasting the revocation message in the network. The size of each group is made large enough that each node has at least *k* nodes in its communication range of about 10 sq miles [30]. Once a certificate is generated by any *k* nodes of the autonomous group, it is transmitted to the other nodes of the autonomous group.

The nodes save the messages that they have sent and received in the ad hoc mode. After the base station is revived, all nodes send their messages to the base station for audit. The base station performs and audit of the messages to ascertain if any of the nodes misbehaved. This audit would determine if any nodes attempted to spread misinformation against the honest nodes or sent positive recommendations for the malicious nodes.

For clear illustration we divide our scheme into 3 stages which are pre ad hoc mode, ad hoc mode and post ad hoc mode. We describe each of these stages in detail.

- **Pre Ad Hoc Mode:** In this stage the nodes are connected to the base station. This stage is performed at regular intervals to provide the latest information for the nodes in the ad hoc mode. The frequency with which the information in the nodes is updated is a tradeoff between overhead and accuracy. In this stage each node receives a reputation score and a share of the private key of the group to which it belongs along with its ID and private key [7]. The ID of each node is a combination of the group ID and the node ID. We represent the ID of a node P with ID_P and the group ID is represented by G_P. The private key corresponding to any ID sent by the base station is represented by SK_{ID}. SK_{G_P}/n is 1 share out of n for the reconstruction of the private key of the group. The communication from the base station can be represented as BS.

  $$BS \rightarrow P : K_s[ID_P \parallel SK_P \parallel SK_{G_P}/n \parallel SCORE_P] \tag{1}$$

  where

  $$SCORE_P = SK_{G_P}[P \parallel Value \parallel timestamp] \tag{2}$$

  The frequency at which this information is updated is a design parameter for the network administrators.
- **Ad Hoc Mode:** The nodes enter this stage when they fail to connect to the base station. Nodes can broadcast messages in this medium using the private keys that they received in the previous stage [7]. When the node P wants to broadcast in this environment it signs the message with its public key and sends the score certificate along with the broadcast.

  $$Sender\colon\ SK_{ID}[M, ID] \parallel ID \parallel SCORE_{ID} \tag{3}$$

  The receivers are able to verify the signature on the message using the ID of the node and they are able to verify the score using the ID of the group to which the sender belongs.

  $$Receiver\colon\ PK_{ID}\big[SK_{ID}[M, ID]\big] \tag{4}$$

  $$Receiver\colon\ PK_{G_{ID}}[ID \parallel Value \parallel timestamp] \tag{5}$$

  Once a receiver believes that a sender is malicious, the receiver sends a negative recommendation to all the anonymous certifiers of the sender. These nodes are all the nodes in the sender's group excluding the sender. When the current certificate of the sender expires, the anonymous certifiers compute a new reputation score based on all the negative recommendations and collaboratively sign the new score with the private key of the group to which the sender belongs. Let R be the receiver and S be the sender.

$$R \rightarrow G_S : SK_R[RECO_R] \parallel ID_R \tag{6}$$

The recommendation itself contains the ID of the recommender, ID of the recommended and the type of recommendation. It is then signed by the private key of the recommender. This is done to ensure the authenticity of the recommender and the recommended. The type of recommendation can have the different levels of positive and negative recommendations that a recommender can make.

$$RECO_R = SK_R[ID_R \parallel ID_S \parallel Value] \tag{7}$$

We understand that the distributed nature of these networks may mean that the recommendations at all the anonymous certifiers may not be the same. Whenever an anonymous certifier reaches a threshold for the negative recommendations, it starts the process of getting the particular node revoked. If there are enough anonymous certifiers which believe that a node needs to be revoked, they can generate a revocation message. There may be a situation where the malicious node broadcasts only one malicious message after which it may not broadcast any other message. To prevent it from broadcasting other messages, the anonymous certifiers can issue no certificate in the future, but that will not discredit the message sent with a malicious certificate. This can be prevented by the anonymous certifiers by broadcasting the revocation certificate in case the reputation score goes below a threshold.

There are many schemes in literature which implement the distributed generation of a signature without any one of the collaborators knowing the signature [31,32]. One of these schemes can be used by the anonymous certifiers to generate the private key of the group without any of the certifiers knowing the actual key.

- **Post Ad Hoc Mode:** Nodes enter this stage when they are able to connect to the base station after the ad hoc mode. In this stage all the messages sent and received in the ad hoc mode by each node are audited. This may also involve the use of the law enforcement agencies to investigate users of the cell phones for the messages that were sent out during the ad hoc mode.

  This stage may be used for correcting any of the trust scores set during the ad hoc mode. Nodes may be rewarded or punished based on their behavior in the ad hoc mode. The recommendations made by the nodes may also be analyzed to determine if a given node is a collaborator of the malicious node. Such nodes may be revoked in the centralized system which is trivial. The post ad hoc node also gives the network administrators an opportunity to correct any mistakes like the revocation of honest nodes, which may have been made in the ad hoc mode. This stage helps in obtaining better reputation scores for nodes when the enter the ad hoc mode in the future.

5. Evaluation

In this section we evaluate the protocol through mathematical analysis and simulations. We first list all the terminology and parameters used in this section. The values of these parameters would influence the security and overhead of this scheme.

- **Group Compromise:** All the nodes of the network are divided into groups. For each node of the group, all the other nodes act as the anonymous certifiers. If the number of malicious nodes in a group is more than the number of nodes required to reconstruct the private key of the group, then the group is said to be compromised.
- **Node Compromise:** When a group is compromised, all the nodes in the group which are not malicious can be revoked. We refer to this as node compromise.
- **Area of Network Deployment:** This is the total area across which the network is deployed. We assume that the communication range of a node is equal in all directions. We represent the deployment region as a circle for clear illustration.
- **Group Size:** It is the number of elements in each group. This is a critical design parameter because for the same level of threshold, if the size of the group is small the probability of there existing a malicious node in the group is also small. On the other hand a small group size reduces the possibility of each node having enough certifiers in its neighborhood.
- **Threshold:** It is the number of anonymous certifiers required to reconstruct the certificate of the group. A lower value of threshold makes the group vulnerable to compromise by a small number of malicious nodes whereas a large value of threshold increases the overhead required for generating a signature. It is also much harder for a node to find enough certifiers to refresh its score certificate.
- **Denial of Service:** Threshold cryptography works when the number of malicious nodes is less than the threshold. But, if the number of malicious nodes in threshold cryptography is large enough such that they are able to prevent the signing of score certificates then the whole system would become dysfunctional. For an (n, k) threshold scheme, the number of nodes required to sign the certificate is k but the number of nodes required to prevent the signing of the certificate is $(n - k)$.

- **Time for Certificate Renewal:** The time for which a certificate is valid is an important design issue. The lifetime of a certificate presents a tradeoff between security and overhead. If the lifetime of a certificate is small, the overhead for signing the certificates on the network would be larger whereas security would be better because the number of broadcasts which can be made by a node is limited.

5.1. Theoretical analysis

We now analyze the probability of a group being compromised which is equivalent to the probability of k out of n nodes of the group being compromised. Let the total number of nodes in the network be N with α being the total malicious nodes in the network. The probability of a particular node being malicious is $\frac{\alpha}{N}$ and the probability of a node belonging to a particular group is $\frac{n}{N}$. The probability of a node being malicious and belonging to a particular group is the product of the two probabilities which is $\frac{n\alpha}{N^2}$. Therefore the probability of k nodes of a group being compromised is

$$P_C = \left(\frac{n\alpha}{N^2}\right)^k \tag{8}$$

This equation presents some interesting results. If the number of nodes in the network increases, the probability of a malicious node belonging to a particular group decreases, which reduces the probability of the group being compromised. An increase in the value of group size would mean that the malicious groups are distributed across fewer groups as a result of which the probability of a group being compromised increases. The most important factor that influences group security is the threshold. A higher threshold would reduce the probability of group compromise exponentially.

We now analyze the problem of Denial of Service in a group. If the number of malicious nodes in a group is less than the threshold value, they will be unable to sign the certificates. But, they can cause DoS by not participating in the signing of score certificates of other nodes of the network. For an (n, k) threshold scheme, if the number of malicious nodes α is greater than $(n - k)$, the group is vulnerable to DoS because without the participation of malicious nodes the honest nodes of the network cannot create signatures. To make this scheme robust to DoS attacks the following conditions have to be satisfied.

$$\alpha \leqslant (n - k) \tag{9}$$

The best possible robustness against DoS is achieved when the group is resilient against $(k - 1)$ malicious nodes. If $\alpha = k - 1$ then

$$k - 1 \leqslant n - k \tag{10}$$

$$\Rightarrow \quad k \leqslant \frac{n-1}{2} \tag{11}$$

If the value of α is greater than q, then the group is compromised.

Let the deployment region have a radius of R and each node have a communication range of r. We assume that the nodes of a group are deployed uniformly throughout the network. Let the density of nodes be ρ. For an (n, k) threshold scheme, the minimum number of nodes within the communication range of a node is k. Therefore the minimum density of nodes required is

$$\rho = \frac{k}{\pi r^2} \tag{12}$$

If the total area of the network is πR^2, the minimum number of nodes required for each group n would be

$$n = k\left(\frac{R}{r}\right)^2 \tag{13}$$

With the increase in the area of deployment, the number of nodes required in each group increases. We believe that the area of the deployment region would be comparable to the communication range of the nodes.

5.2. Simulation results

We have also simulated the different aspects of this paper. The simulations bring out the relations between the different aspects of this paper.

In Fig. 2 we present the basic principle of threshold cryptography. It shows the relation between threshold, overhead and risk. As the threshold increases, the overhead required to reconstruct the shared secret increases. Each node has to generate a partial signature to the score certificate which is then combined to generate the final score certificate. As a result overhead is directly proportional to the threshold. Risk on the other hand is inversely proportional to threshold. If the threshold is 1, the risk is the highest. As the value of threshold increases, the number of nodes which are required to sign the certificate

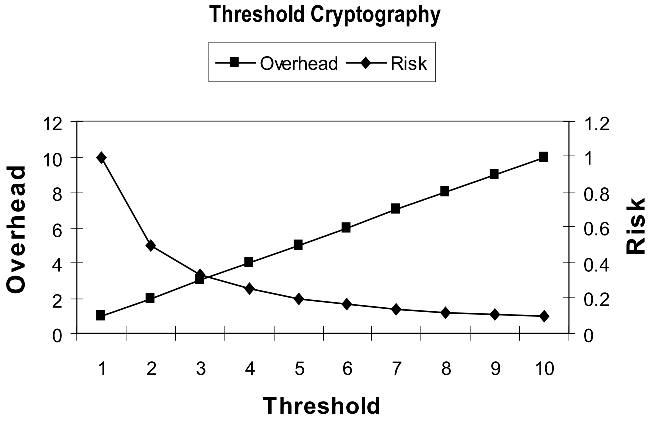

Fig. 2. This figure shows the relation between threshold, overhead and risk in threshold cryptography. As the threshold increases the risk decreases and overhead needed to reconstruct the secret increases.

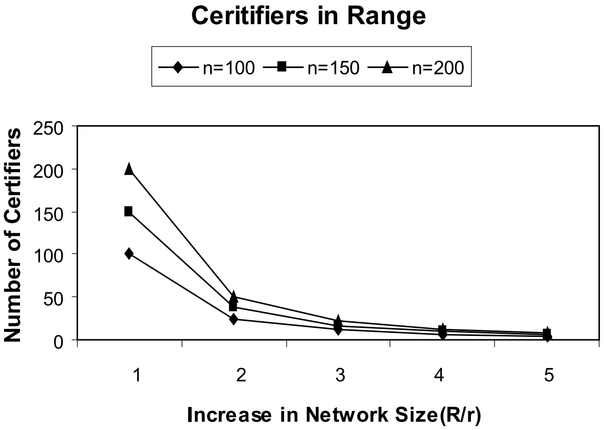

Fig. 3. This figure shows the relation between the number of anonymous certifiers within communication range and the area of network deployment. r/R indicates the ratio of the radius of the deployment region to the communication range of a node.

increases. This is clearly illustrated in Fig. 2. In this figure we assume that each node of the network has only share of the group private key. If the use of some pre trusted nodes like cops are made, the risk of threshold cryptography can be lowered.

In Fig. 3 we show the relationship between the network size and the number of nodes which are within communication range. The communication range of each node is assumed to be constant. The area of deployment is assumed to be circular and represented in terms of the communication range of each node. This simulation assumes that there are 10 000 nodes in the network and the number of anonymous certifiers are distributed uniformly throughout the network. We can clearly see that with the increase in the area of the network, the number of anonymous certifiers decreases dramatically. We believe that in a real world implementations the sizes of the groups would be very large compared to the threshold size to be able to cover a reasonably large deployment area. We also believe that the size of the ad hoc network would be comparable to the communication range of the nodes.

In Fig. 4, we present the relationship between the number of nodes compromised when a certain number of nodes are malicious for different values of group size. A node is compromised when at least k nodes of its group are malicious. In this simulation, the number total number of nodes is taken as 10 000. We perform this simulation for different values of the group sizes. All the values in Fig. 4 are represented as a percentage of the total nodes in the network. When the number of malicious nodes is small, an increase the number of malicious nodes does not compromise honest nodes because the number of malicious nodes in all groups is less than the threshold. As the number of malicious nodes increases, the number of groups in which the number of malicious nodes is greater than the threshold increases suddenly. This figure shows that as long as the number of malicious nodes is small compared to the total nodes (around 1–2%), the number of nodes compromised is negligible. Fig. 4 also shows that an increase in group size increases the number of groups compromised for a given level of malicious nodes. This behavior is expected because when the group size is increased and the threshold

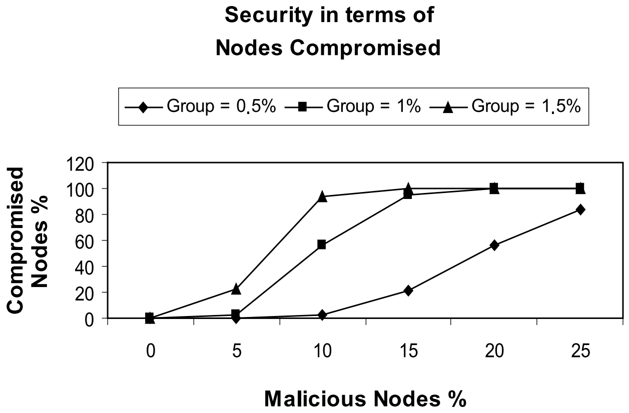

Fig. 4. An increase in the number of malicious nodes increases the number of nodes compromised. An increase in group size causes the number of malicious nodes are spread across fewer groups. Hence the rapid increase in nodes compromised. Values are represented as fractions of total nodes.

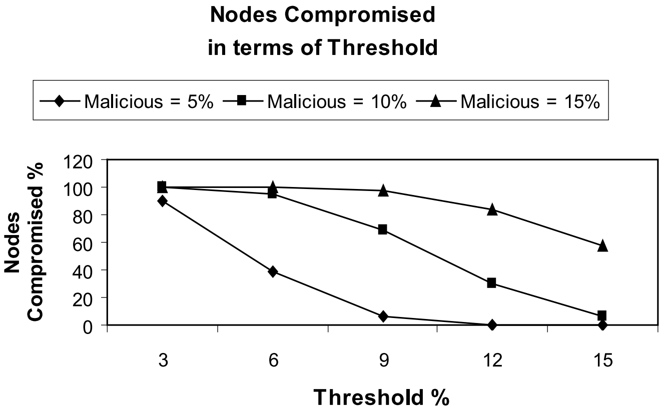

Fig. 5. This figure shows the relation between the nodes compromised and the threshold. As the threshold increases the value of nodes compromised decreases. The nodes compromised and malicious nodes are a fraction of the total nodes of the network whereas the threshold is a fraction of group size.

is kept constant, the malicious nodes are spread across fewer groups. As a result the number of malicious nodes in each group is higher and the number of malicious nodes reaches the group threshold faster.

In Fig. 5, we present the relationship between the nodes compromised and the threshold. Intuitively, an increase in the value of threshold would result in better security and thus, fewer compromised nodes. In this figure, threshold is represented as a fraction of the group size whereas the nodes compromised and the malicious nodes are represented as fractions of total nodes in the network. For this simulation, the group size was taken as 100 and the network size was taken as 10 000. For a high value of malicious nodes at 5%, a threshold of 15% of group size achieves zero compromised nodes. We believe that in such networks the number of malicious nodes would be negligible when compared to the total nodes in the network.

6. Conclusions

We presented a distributed scheme for reputation management in an ad hoc network of cell phones. The nodes of this network, cellular phones, are able to communicate with each other when the nodes are unable to connect to the base station of the ad hoc network. In this operating environment our earlier paper had developed a key distribution scheme for the ad hoc mode using the secure cellular infrastructure [7].

Each node of this network is assigned a reputation score based on various factors like criminal record, credit history etc. We presented a scheme which not only alters the reputation score based on the recommendations of other nodes of the network but also revokes the nodes when this score goes below a certain threshold. This is achieved by dividing the nodes into different groups such that each all the elements of a group act as the anonymous certifiers for a node. Each group has a key which is distributed across all the nodes of the group. This key is used to sign score certificates for individual nodes in such a way that no one node knows the secret. This key is also used to sign the revocation message which is broadcasted throughout the network. In this paper, we analyzed the factors which would help the network administrator fine tune this scheme.

References

[1] Cellular News, USA saw lowest ever annual subscriber growth in 2008, Online Article (2009), http://www.cellular-news.com/story/36734.php?s=h.

[2] J. Cai, D.J. Goodman, General packet radio service in GSM, IEEE Commun. Mag. (October 1997) 122–131.

[3] L. Buttyan, J.-P. Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks, Mob. Netw. Appl. 8 (5) (2003) 579–592, http://dx.doi.org/10.1023/A:1025146013151.

[4] L. Mui, M. Mohtashemi, A. Halberstadt, A computational model of trust and reputation for e-businesses, in: HICSS'02: Proceedings of the 35th Annual Hawaii International Conference on System Sciences, HICSS'02, vol. 7, IEEE Computer Society, Washington, DC, USA, 2002, p. 188.

[5] J. Liu, V. Issarny, Enhanced reputation mechanism for mobile ad hoc networks, in: iTrust, 2004, pp. 48–62.

[6] P. Obreiter, A case for evidence-aware distributed reputation systems — overcoming the limitations of plausibility considerations, in: Second International Conference on Trust Management, iTrust'04, Oxford, UK, 2004, http://citeseer.ist.psu.edu/obreiter04case.html.

[7] A. Durresi, V. Bulusu, V. Paruchuri, Secure emergency communication of cellular phones in ad hoc mode, J. Ad Hoc Networks 5 (1) (2007) 126–133.

[8] P. Traynor, P. McDaniel, T.L. Porta, Security for Telecommunications Networks, vol. 233, Springer Science + Business Media, Spring Street, New York, NY 10013, USA, 2008.

[9] SMS over SS7. Technical Report Technical Information Bulletin 03-2, Tech. Rep. NCS TIB 03-2, National Communications System, December 2003.

[10] S.P. Marsh, Formalising trust as a computational concept, PhD thesis, University of Stirling, April 1994, http://www.cs.stir.ac.uk/research/publications/techreps/pdf/TR133.pdf.

[11] Y. Ren, A. Boukerche, Modeling and managing the trust for wireless and mobile ad hoc networks, in: ICC, IEEE, 2008, pp. 2129–2133, http://dx.doi.org/10.1109/ICC.2008.408.

[12] S. Zhong, J. Chen, Y.R. Yang, Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks, in: INFOCOM, 2003.

[13] T. Repantis, V. Kalogeraki, Decentralized trust management for ad-hoc peer-to-peer networks, in: S. Terzis (Ed.), MPAC, in: ACM International Conference Proceeding Series, vol. 182, ACM, 2006, p. 6, http://doi.acm.org/10.1145/1169075.1169081.

[14] V. Cahill, E. Gray, C. Jensen, J.-M. Seigneur, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nicon, Using trust for secure collaboration in uncertain environments, IEEE Pervasive Comput. 2 (3) (2003) 52–61.

[15] K. Kane, J.C. Browne, Using uncertainty in reputation methods to enforce cooperation in ad-hoc networks, in: R. Poovendran, A. Juels (Eds.), Workshop on Wireless Security, ACM, 2006, pp. 105–113, http://doi.acm.org/10.1145/1161289.1161308.

[16] A. Jøsang, An algebra for assessing trust in certification chains, in: Proceedings of the Network and Distributed Systems Security Symposium, NDSS'99, Internet Society, 1999.

[17] F. Li, J. Wu, Mobility Reduces Uncertainty in MANETs, in: Proceedings of 26th IEEE International Conference on Computer Communications, INFOCOM 2007, Anchorage, AK, USA, 2007, pp. 1946–1954.

[18] A. Jøsang, J. Golbeck, Challenges for robust of trust and reputation systems, in: Proceedings of the 5th International Workshop on Security and Trust Management, STM 2009, Saint Malo, France, 2009.

[19] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, Propagation of trust and distrust, in: Proceedings of the 13th International Conference on World Wide Web, ACM Press, New York, NY, USA, 2004, pp. 403–412.

[20] V. Balakrishnan, V. Varadharajan, U. Tupakula, Chapter 19: Trust Management in Mobile Ad Hoc Networks, Springer, London, 2009, pp. 473–502.

[21] A. Jøsanga, R. Ismailb, C. Boydb, A survey of trust and reputation systems for online service provision, Decision Support Systems 43 (2) (2007) 618–644.

[22] A. Durresi, V. Paruchuri, L. Barolli, Trust management in emergency networks, in: Proceedings of the International Conference on Advanced Information Networking and Applications, AINA2009, Bradford, UK, 2009, pp. 167–174.

[23] M. Kinateder, K. Rothermel, Architecture and algorithms for a distributed reputation system, in: P. Nixon, S. Terzis (Eds.), Proceedings of the First International Conference on Trust Management, in: Lecture Notes in Comput. Sci., vol. 2692, Springer-Verlag, Crete, Greece, 2003, pp. 1–16, http://citeseer.ist.psu.edu/kinateder03architecture.html.

[24] M. Virendra, S. Upadhyaya, Securing information through trust management in wireless networks, in: Workshop on Secure Knowledge Management, SKM 2004, Buffalo, NY, September 2004, pp. 201–206.

[25] L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network 13 (6) (1999) 24–30, http://citeseer.ist.psu.edu/zhou99securing.html.

[26] C.R. Davis, A localized trust management scheme for ad hoc networks, in: Proceedings of 3rd International Conference on Networking, ICN'04, March 2004, pp. 671–675.

[27] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, J. Cryptology 17 (4) (2004) 297–319, http://dx.doi.org/10.1007/s00145-004-0314-9.

[28] A. Shamir, Identity-based cryptosystems and signature schemes, in: Proceedings of CRYPTO 84 on Advances in Cryptology, Springer-Verlag, New York, NY, USA, 1985, pp. 47–53.

[29] A. Fernandes, E. Kotsovinos, S. Ostring, B. Dragovic, Pinocchio: Incentives for honest participation in distributed trust management, in: Proceedings of the 2nd International Conference on Trust Management, iTrust, 2004, Oxford, UK, 2004, pp. 63–77, also published in Springer-Verlag Lecture Notes in Computer Science (LNCS), vol. 2995, pp. 63-77.

[30] J. Layton, M. Brain, J. Tyson, Introduction to how cell phones work, 2005, http://electronics.howstuffworks.com/cell-phone.htm.

[31] Y. Desmedt, Y. Frankel, Shared generation of authenticators and signatures (extended abstract), in: CRYPTO'91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, Springer-Verlag, London, UK, 1992, pp. 457–469.

[32] Y.G. Desmedt, Y. Frankel, Threshold cryptosystems, in: CRYPTO'89: Proceedings on Advances in Cryptology, Springer-Verlag, New York, NY, USA, 1989, pp. 307–315.