www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1812-1819

HIERARCHICAL WITH STRONG AUTHENTICATION REDUCTION SCHEME IN MANETS

D.M.D.Preethi
Assistant Professor
,Department of computer science and Engineering
P.S.N.A. College of Engineering and Technology
Dindigul
dmd_p@rediffmail.com

Abstract

Many existing reputation systems sharply divide the trust value into right or wrong, thus ignoring another core dimension of trust: uncertainty. As uncertainty deeply impacts a node's anticipation of others' behavior and decisions during interaction. Besides lacking a precise semantic, this information has abstracted away any notion of time. This approach is objective and robust. But, this approach still leaves an opportunity for elaborate attackers to launch false accusation attacks since there is no constraint on update frequency. This approach also lacks the ability to separate newcomers from misbehavers.. Uncertainty originates from information asymmetry and opportunism. It reflects whether a trustor has collected enough information from past interactions with a trustee and its confidence in that information. So in this paper the concept of uncertainty and its role in trust evaluation. It Propose a certainty-oriented reputation system. This present various proactive and reactive mobility assisted uncertainty reduction schemes.

Keywords-uncertainty, reputation, strong authentication

I. Introduction

In reputation system, one cannot verify exact properties of past behavior based on the information alone. To solve this problem, uncertainty is used to evaluate the trust.uncertainty refers to the degree to which an individual or organization cannot accurately predict the behavior of its mutual rival or the environment. One way to reduce uncertainty is to exploit one important property Of manet is mobility. Node movement can increase the scope of direct interaction and recommendation propagation, thereby speeding up trust convergence.

The procative schemes aim to disseminate local reputation. Information by nodes movement and achieve a global trust convergence.in which, mobile nodes build up trust relartionships,collect trust information, move, and disseminate the collect information through recommendation. The reactive schemes focus on the dispatching mobile ambassadors to authenticate moving nodes and forward the moving nodes original reputation to the new destination through recommendation.Both schemes illustrate positive impacts of mobility on uncertainty reduction and offers a a flexibilty.

II.Calculation and Update of Reputation Values

A. Trust vs. Reputation

Applied to mobile ad hoc networks, reputation can be defined as one node's perception of another Node's performance of some network operation. It is used as a prediction of future quality of service. However, since reputation is not a tangible property, the reputation value has to be explicitly defined. There are some issues that should be considered during the calculation and update of the reputation value.

B. Direct vs. Indirect Trust (Reputation)

Direct reputation is derived from first hand experience. A node gets such information about another node, usually its one-hop neighbor, by direct observation. For example, node M forwards a message (either a routing message or a data packet) to its next hop neighbor, N, and expects N to further forward the message. M can get first hand information by monitoring whether N correctly participates in the protocol.

Indirect reputation information (also refers to second hand reputation information) is reputation information about a node from other nodes. Such reputation information can be in the form of a blacklist, friends list or a

reputation table. It may be first hand information of the sender or may be transmitted hop-by-hop from the originator. We can model trust and reputation as follows: Direct trust and reputation are based on direct knowledge or observation. Trust and reputation may not be symmetric. For example, if node A knows that node B to be trustworthy, this does not imply that B knows that A is trustworthy. Trust and reputation are usually assumed to be transitive .For example, if node A knows that node B is trustworthy and node B knows that node C is trustworthy, then node A can trust C.

Indirect trust and indirect reputation are based on trust and reputation that link nodes. For example, if node A trusts node B is trustworthy and node B trusts node

C, then A trusts C. On the other hand, if node A does not trust node B, then A will not trust C even if B trusts C. A node A can know something about another node C from the indirect reputation message if and only if A knows the indirect reputation information is from a trustworthy node B.

C Global vs. Local reputation

Most reputation systems for mobile ad hoc network uses global reputation, in which every node knows reputation of every other node in the network. This is achieved by exchange indirect reputation messages among the network. Since indirect reputation information may be from an untrustworthy node, reputation systems using global reputation information suffer from false rating, either false accusation or false praise.

D. Initiate Reputation Value

When a new node enters the network, or a node moves to a new location, where nobody knows about its reputation, an initial reputation value should be given. Each reputation system has a learning period, as the network will not know how a new node will behave. Assign the lowest possible reputation value to a new node will force it to perform positive work to gain a good reputation, and thus discourage new participants from malicious behavior. But this mechanism may not be feasible in an ad hoc network, where instantaneous connection is required and nodes are more mobile. It may take too much time for a new node to establish its reputation.

E. Inconsistent Reputation Value

In reputation systems, different nodes may have different reputation values for the same node. This is called the inconsistent reputation problem. It may be caused by many reasons. Nodes may calculate reputation values differently.

The reputation mechanisms usually assume that every node will assign the same weights to the functions. This is a potentially inappropriate assumption in a mobile ad hoc network, where nodes with different capabilities and roles are likely to place different levels of importance on different functions For different nodes, first hand reputationvalues of a same node may vary. Every node gets firrst hand reputation information about nodes that it interact with based on its own experience. A node may behave differently when interact with different nodes, thus the reputation value for a same node may vary. For example, two nodes, A and B both interact with node C, but A and B may have different reputation values for C. This is possible if C react differently to request from A and B; or A or B may interact with C often than the other. Every node deals with the received indirect reputation information .based on its own judgement.This also results in the difference Reputation information accepted by node A may not be accepted by node B because it is either incompatible with B's experience or B does not trust the sender. None of the reputation methods discussed above require nodes in a mobile ad hoc network to reach a consensus on which nodes misbehave.

III. Security and trust

A. Trust and reputation systems as soft security mechanisms

The purpose of security mechanisms is to provide protection against malicious parties.In this sense there is a whole range of security challenges that are not met by traditional approaches. Traditional security mechanisms will typically protect resources from malicious users,by restricting access to only authorized users.

B .Computer security and trust

The concepts of trusted systems and trusted computing base have been used in IT security, but the concept of security assurance level is more standardized as a measure of security.

C .Communication security and trust

Communication security includes encryption of the communication channel and cryptographic authentication of identities. Authentication provides so-called identity trust,i.e a measure of the correctness of a claimed identity over a communication channel. The term “trust provider” is some times used in the industry to describe CA_S and other authentication service providers with the role of providing

the necessary mechanisms and services for verifying and managing identities.

IV. Reputation network architecture

The network architecture determines how ratings and reputation scores are communicated between participants in a reputation system .The two main types are centralisd and distributed architecture.

A. Centralized reputation systems

In centralized systems, information about the performance of a given partipant is collected as ratings from other members in the community who have had direct experience with that participant. The central authority (reputation center) that collects all the ratings typically derives a reputation score for every participant, and makes all scores publicly available Participants can then use each other's scores,for example, when deciding whether or not to transact with a particular party.The idea is that transactions with reputable participants are likely to result in more favorable outcomes than transactions with disreputable participants.

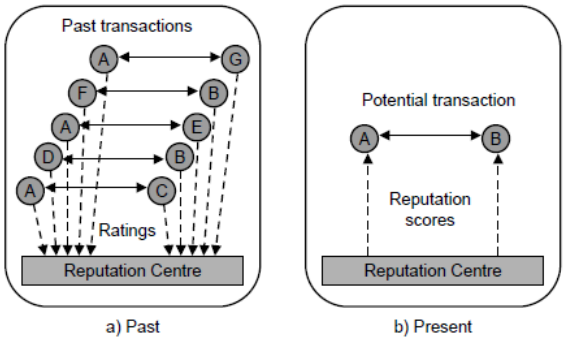

Fig.1. General framework for a centralized reputation system

After each transaction, the agents provide ratings about each other's performance in the transaction. The reputation centre collects ratings from all the agents and continuously updates each agent's reputation score as a function of the received ratings. Updated reputation scores are provided online for all the agents to see, and can be used by the agents to decide whether or not to transact with a particular agent. The two fundamental aspects of centralized reputation systems are:

1. Centralised communication protocols that allow participants to provide ratings about transaction partners to the central authority, as well as to obtain reputation scores of potential transaction partners from the central authority.

2. A reputation computation engine used by the central authority to derive reputations cores for each participant, based on received ratings, and possibly also on other information.

B. Distributed Reputation Systems

There are environments where a distributed reputation n system, i.e. without any centralized functions, is better suited than a centralized system. In a distributed system there is no central location for submitting ratings or obtaining reputation scores of others. Instead, there can be distributed stores where ratings can be submitted, or each participant simply records the opinion about each experience with other parties, and provides this information on request from relying parties. A relying party ,who considers transacting with a given target party, distributed stores, or try to obtain ratings from as many community members as possible who have had direct experience with that target party. This is illustrated in this figure below.

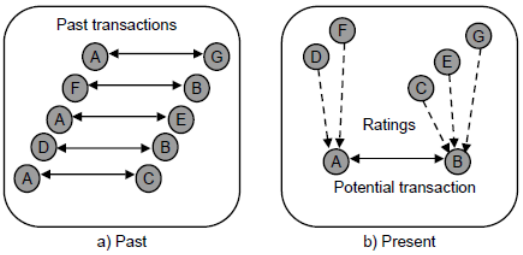

Fig. 2. General framework for a distributed reputation system

The relying party computes the reputation score based on the received ratings. In case the relying party has had direct experience with the target party, the experience from that encounter can be taken into account as private information, possibly carrying a higher weight than the received ratings.

The two fundamental aspects of distributed reputation systems are:

1. A distributed communication protocol that allows participants to obtain ratings from other members in the community.

2. A reputation computation method used by each individual agent to derive reputation scores of target parties based on received ratings, and possibly on other information .Peer-to-Peer (P2P) networks represent a environment well suited for distributed reputation management.

The purpose of a reputation system in P2P networks is:

1. To determine which servents are most reliable at offering the best quality resources, and

2. To determine which servents provide the most reliable information with regard to (1).

In a distributed environment, each participant is responsible for collecting and combining ratings from other participants. Because of the distributed environment, it is often impossible or too costly to obtain ratings resulting from all interactions with a given agent. Instead the reputation score is based on a subset of ratings, usually from the relying party's neighbourhood.

V.Hierarchical algorithm

The hierarchical scheme consists of the following three parts. Moving node election. After the cluster has been set up, all the nodes in the cluster will contact each other locally,build up trust, and compute reputation according to thepreviously discussed reputation system. After a sufficient pause time, each node will vote for the node with the largest belief and smallest uncertainty to move. The voting process can be described as Algorithm 1. Here, Bmin is the belief threshold. _ is the required proportion of votes to win an election. Umax, Bmin, and _ should be regulated in the clusters' voting policy and represent the reputation requirements for a moving node. Each node sets a pause timer and will cast only one vote after time-out.

Algorithm 1. VoteForMove
1: while the timer lasts do
2: Get first-hand observation and change _; _ accordingly when an event occurs;
3: Update second-hand opinion accordingly when a recommendation comes;
4: end while
5: Compute combined opinion b; d; u for each node;
6: if the largest b in all the opinions satisfy b _ Bmin then
7: Vote the node with the largest b;
8: Wait for the confirmation from elected moving node;
9: else
10: Continue trust information collection;
11: end if;
. Each region selects one grid to be its capital. All of the elected moving nodes move to the capital of the region.

Algorithm 2. VoteGathering

1: Vote counter+1 when a vote comes;
2: if vote counter _ _ proportion of the nodes in the cluster then
3: Node broadcasts an elected confirmation and starts to move;
4: end if;

The moving nodes repeat the local contact process after they arrive in the capital.
Region partition. The election process creates different roles to handle different trust information collection and dissemination tasks for intragrid, intra region, and inter region.

Our proactive algorithm implements a multi-path version of Bellman-Ford routing. Since it needs to function as a lightweight background process, it is designed to work efficiently under all circumstances. In what follows, we first describe the general working of the algorithm, and then give details about the routing information update process and the loop avoidance mechanism.

General working of the proactive algorithm

The basic working of the algorithm is as follows:

1. Each node i in the network maintains a routing tableTi, with an entry t dij for each known destination d andeach next hop j. t dij contains an estimate cdij of the cost of the route towards d over next hop j (estimations of link and route costs are based on the number of hops and the signal strength over the links).

2. At periodic intervals (set to 1 s), node i broadcasts an update the e message containing for maximum of the destinations in its routing table the best routing estimate cdij = min j∑Ni(cdij) taken over all next hops j in its set of neighbors Ni (if it does not have a routing estimate to a previously known destination, it indicates a cost of infinity). m is a constant that limits the size of update messages (set to 20 in our tests). If there are less than m destinations, they are all are included in each message. Otherwise, update messages include subsets of m destinations selected in a round-robin fashion.

3. Each neighbor k of node i receive the update message, and use it to calculate for each of the destinations d its own new estimate cd ij for the cost of the route over next hop i to d. It does so by adding the estimate c iˆd received from i to the estimated cost of going from k to i.

The routing information update process

The main difference between our proactive algorithm and other Bellman-Ford routing algorithms (such as lies in the way routing updates are spread. We only use periodic update messages that are limited in size. This means that routing overhead is not influenced by the occurrence of disruptive events, as no extra routing information is generated to deal with them (contrary to DSDV, where substantial changes are broadcast faster). It also means that routing overhead is not dependent on the network size: if the number of destinations exceeds m, information about them is spread over multiple subsequent update messages. In terms of implementation, routing

update messages are piggy-backed on top of beacon messages.

Loop avoidance

The loop avoidance mechanism is based on sequence numbers, similar to DSDV. However, since DSDV is a single path algorithm while ours is multi-path, we use sequence numbers in a different way. The main idea is to have all destination nodes issue sequence numbers and spread these together with the routing information, and to let data packets only follow routes of increasing sequence numbers or decreasing costs. The general working is as follows:

1. Each node i maintains a local sequence number si.It also maintains in each routing table entry t dij a sequence number s ijd , which is the last sequence number received for destination d over next hop j. Finally, it maintains for each destination d a sequence number $s^{d}i$, which is the highest sequence number i has broadcast for d in its update messages, and a cost value c_i^{d} , which is the lowest cost broadcast for d related to this sequence number.

2. For each periodic routing update message, i increments the local sequence number s^{i} by 1 and includes it in the message. Then, it adds the best routing information for each destination d to the update message (as described earlier), and adds to this the sequence number s ijd related to the best next hop j towards d. Finally, it updates s di , its local record of the highest sequence number it has broadcast for destination d, and the associated lowest cost ci d as follows: if s d i < s ijd , s di is set to s ijd and ci d is set to cij d ; otherwise, if s di = s ijd and ci d > cij d , ci d is set to cij d .

3. A node j receiving an update message from i storesthe sequence number si in its routing table entry t iij as s iij , the last sequence number received for destination i over next hop i. Then, for each destination d mentioned in the update message, it sets sd ij to the received sequence number.

4. Data packets arriving in a node i for a destination dare only forwarded to a next hop j if s ijd > s di (thesequence number for d related to j in i is higher than the highest that i has broadcast for d), or if s ijd = s di and cijd <= c di (the sequence number for j is the same as the highest i has broadcast and the cost for j is equal or lower than the lowest i has broadcast for this same sequence number).

The reactive algorithm

In the simple authenticated selection scheme, when a node is about to move to a destination region, it will inform the CH of its home region about its destination. The CH checks the following conditions and decides whether to assign the outgoing node i the duty of ambassador: 1) Rep_i _ T, 2) the public key of i is properly stored, and 3) no record indicates that a valid ambassador exists in the intended destination region of node i. Here, we use Rep_i to represent node i's reputation in the home region, and T is the threshold of reputation which represents the CH's requirement for its ambassadors. These conditions are the basic requirements for ambassadors, which are also adopted by the following three schemes. When searching for the ambassadors, the moving node only investigates its home region for an ambassador of the destination region. If it cannot find the ambassador, it directly moves to the destination. If the moving node found an ambassador of the destination region in its home region, the ambassador generates a certificate as the visa. This process is illustrated in the following figure.

5

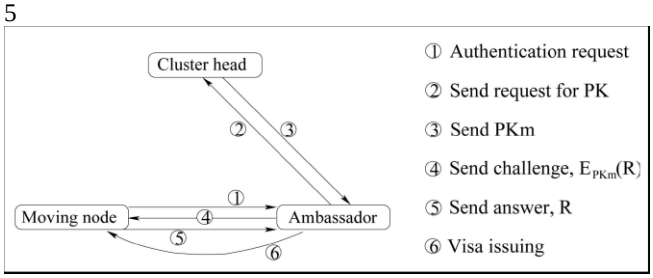

Fig3Authentication process

In this visa, the ambassador should include node i's public key PK_i, i's reputation in the home region Rep_i, and signed by the cachet key CK from the ambassador's home region visa ¼ $E_{CK}fPK_ijRep_ig$.

Here, E_{CK} means encrypting by CK.

The moving node takes this visa to its destination region. Upon arrival, it presents the visa to the CH in the destination region. The CH verifies the visa, broadcasts the moving node's public key, and announces its reputation as the initial reputation of the moving node in the region.

The reactive algorithm provides a connection-oriented routing service. At the start of a data session, it executes a route setup to build an initial route. During the course of the session, it applies route improvement mechanisms to adapt the current route to changes in the MANET. Finally, it has mechanisms to deal with link failures.

Strong authentication

Strong authentication is defined as validation of a node's identity against previously stored information using cryptographically derived credentials. Ad hoc networks are prone to eavesdropping, so identity information and all cipher keys (public, private, or shared keys) of the nodes should be encrypted to protect against cyber adversaries. An authentication protocol must not rely on a centralized server for key distribution, because in that case it will be a weak link in the network and thus becomes the limiting element in the availability of the network. Moreover, the network topology and architecture are dynamically reconfigurable because the nodes are mobile

Components of a strong authentication process

The general procedure of strong authentication in MANETs. There are six steps for a strong authentication solution: bootstrapping, pre-authentication, credential establishment, authentication, monitoring, and revocation as shown in the flowchart of Figure 3. It is a three-stage framework: pre-authentication, authentication, and session key establishment for subsequent data communications

An authentication protocol is a sequence of message exchanges between supplicants and authenticators that distributes credentials and allows the use of the credentials to be recognized. "A Trusted Third Party (TTP) is an entity that is mutually trusted by the supplicant and the authenticator and that can facilitate mutual authentication between the two parties.

"1) Bootstrapping is a step when a supplicant establishes a credential, either offline or online. The credential may be something that it has (e.g., key), something it knows (e.g., password),or something it is (e.g., biometric). For example, bootstrapping may be performed by assigning an initial global key to each new node joining a network .

2) Pre-authentication is the step when a supplicant presents its credential(s) to an authenticator in an attempt to prove its eligibility to access protected resources or offer services.

3) Credential establishment: This step establishes the supplicant's new credentials, which the system will use as proof of its identity and as a verification of its authorized state thereafter. A credential could be a symmetric key, a public/private key pair, a commitment of a hash key chain, or some contextual information.

6) Revocation: This step covers two main issues: 1) when should a node be put on the revocation list, 2) how can the revocation be broadcast to all nodes.

.

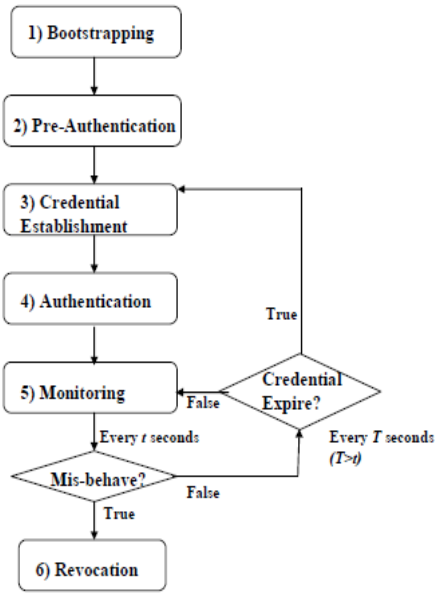

Fig4.Components of a strong authentication process

4) Authentication: In this step, the communication between the supplicant and the authenticator is validated at the destination using the established credentials. Upon success of all of the steps above, a supplicant is considered authenticated, which means that it is authorized to access resources protected by the authenticator.

5) Monitor: While authenticated, a supplicant's behavior is monitored to ensure it is neither compromised nor "misbehaving", a term used for internal adversaries. A compromised supplicant may get its credentials revoked/isolated.

Lightweight Integrated Authentication (LIA) Scheme

We propose a cooperative and distributed authentication architecture for tactical MANETs that is intended to address eight of the requirements listed in section 3.3 and include the six steps. The proposal integrates user-to-device and device-to-network authentication and focuses on distributed detection, This integrated authentication scheme may also be used with PKI encryption; however, it will not be as "lightweight

Step 1: Bootstrapping: An off-line PKG generates private keys for all nodes, based on their identities, with a master secret key. The PKG would no longer be involved in the wireless network after the private keys have been issued. However, upon expiry or revocation, only the PKG can renew or regenerate private keys.

Step 2: Pre-authentication: Using its private key and the identity of its recipient node (public key), every node can compute its pair-wise symmetric key for communicating to

another. This assumes that the identities are known to the users.

Step 3: Credential Establishment: The pair-wise symmetric keys are shared between two nodes.
Step 4: Authentication: Mutual authentication is performed when the two nodes compare their pair-wise symmetric keys.
Step 5: Monitoring: The system is self monitored because the user-to-device authentication is integrated into device-to-network authentication. It is used to perform user-to-device authentication through wearable biometric sensors [because they have the potential to have the following properties: 1) direct user binding for sufficient security, 2) non-disruptive re-authentication, 3) high accuracy with low false rejection rate, 4) low energy consumption, and 5) low computation complexity.

Step 6: Revocation: We propose that a distributed entity called the Revocation Authority (RA) revoke compromised (or expired) keys. The RA could be netted through the MANET via a covert channel.

PKI-based Integrated Authentication (PIA) Scheme

PKI also satisfies , starting with the required six steps.

Step 1: Bootstrapping: The same as LIA where a CA replaces a PKG. An off-line CA generates public and private keys for all the nodes. The CA would no longer be involved in the wireless network after the keys have been issued. However, upon revocation, only the CA can renew or regenerate keys.

Step 2: Pre-authentication: Using its own private key, a node encrypts a document for the recipients.

Step 3: Credential Establishment: The recipients decrypt the document using the sender's public key. This assumes that the public keys are known to the users.

Step 4: Authentication: One-way authentication is formed when the recipient node · is able to successfully decrypt the document with the sender's public key – a sign of bound authenticity to the private key – and · compares the document (or its hashed version) with that of it's own. The document is usually a signed certificate by the TTP – a sign of trust due to belonging to the same CA. For mutual authentication, both nodes should perform the one-way authentication process.

Step 5: Monitoring: The same as LIA.

Step 6: Revocation: The same as LIA.

Once the public and private keys are in place with the bootstrapping step, every node can exchange a generated symmetric key for subsequent encryption of information to another. The sender generates a symmetric key and attaches it to a PKI-encrypted message. This assumes that the public keys are known to the users. The sender can continue its secure information exchange to the receiver(s) by encrypting with the symmetric key. In this manner, the key exchange is secured with PKI, and the information exchange remains efficient with a symmetric key.

Analysis:

Hierarchical with strong authentication schemes offer many ways to adjust the trust convergence delay and cost related to a specific certainty goal. We analyze the trade-offs between delay, cost, and uncertainty in different mobility-assisted uncertainty reduction schemes, so as to provide flexible and controllable methods to support reputation-based applications in MANETs.

Conclusion

In this paper uncertainty can be reduced by,with the use of hierarchical with strong authentication scheme. Mobile nodes are strongly authenticated .proactive and reactive scheme offer flexibility for users to achieve application specific goals. Strong authentication can be realized by integrating user-to-device authentication with device-to-network authentication because the user and the device are generally tightly coupled in tactical MANETs. Benefit of this integration is its efficiency for secure network access control because user authentication is decoupled from, and distributed to, devices and it does not consume precious network bandwidth in MANETs.

Acknowledgments

This paper is substantially extended version for Uncertainty Modeling and Reduction in MANETs Feng Li and Jie Wu and Strong Authentication for Tactical Mobile Ad Hoc Networks Helen Tang, Mazda Salmanian and Connie Chang.

References

[1] Feng Li, and Jie,"Uncertainty Modeling and Reduction in MANETs", IEEE transactions on mobile computing, vol. 9, no. 7, july 2010.
[2] A. Josang, "An Algebra for Assessing Trust in Certification Chains," Proc. Network and Distributed Systems Security Symp. (NDSS '99), 1999.
[3] A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.
[4] W. Zhang, S. Das, and Y. Liu, "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks," Proc.Ann. IEEE comm. Soc. Sensor and Ad Hoc Comm. and Networks, 2006.
[5] S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," Proc. Int'l Symp. Mobile Ad Hoc Networking and Computing, 2002.
[6] M. Carbone, M. Nielsen, and V. Sassone, "A Formal Model for Trust in Dynamic Networks," Proc. IEEE Int'l Conf. Software Eng. and Formal Methods (SEFM '03), 2003.

[7] A. Josang, S. Marsh, and S. Pope, “Exploring Different Types of Trust Propagation,” Proc. Int’l Conf. Trust Management, 2006. [8] A. Josang and S. Pope, “Normalising the Consensus Operator for Belief Fusion,” Proc. Int’l Conf. Information Processing and Management of Uncertainty, July 2006.
[9] T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Comm. and Mobile computing, vol. 2, no. 5, pp. 483-502, 2002.
[10] Genik, L., Salamanian, M., Schotanus, H., Hansson, E., Verkoelen, C., Mason, P., 2004.Mobile Ad Hoc Network Security from a Military Perspective. DRDC Ottawa TR 2004-252, Defence R&D Canada – Ottawa.
[12] Helen Tang, Mazda Salmanian and Connie Chang “Strong Authentication for Tactical Mobile Ad Hoc Networks”Defence R&D Canada, Ottawa technical memorandum, July 2007.
[11] LVenkatraman, and D.Agrawal., “A Novel Authentication Scheme for Ad HocNetworks.” In IEEE Wireless Communications and Networking Conference (WCNC2000), vol. 3, pp. 1268--1273, 2000.