Hcm-Ambassador Dispatching And Seeking Methods In Manets

D. M. D. Preethi

Department of Computer Science and Engineering
PSNA College of Engineering and Technology
Dindigul , India

Abstract

Uncertainty deeply impacts a node's anticipation of others' behavior and decisions during interaction. 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. is approach also lacks the ability to separate newcomers from misbehavers.. The main challenge in MANETs arises from their self-organized and distributed nature. Mobile ad hoc networks (MANETs) aim to provide network services without relying on any infrastructure. Mobility is the important characteristics of MANETs, to efficiently reduce uncertainty and to speed up trust convergence. So in this project uncertainty be reduced the dispatching scheme with the strong authentication .

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 source to the new destination through recommendation.Both schemes illustrate positive impacts of mobility on uncertainty reduction and offers a flexibility.

II. Background for trust and reputation systems

A.*The notation of trust*

Definition 1(Reliability Trust):Trust is the subjective probability by which an individual. A expects the another individual ,B, performs a given action on which its welfaredepends.

Definition 2(Decision Trust)**:** Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security,even though negative consequences are possible.

B.Reputation and Trust

Definition 3(Reputation): Reputation is what is generally said or belived about a person's or thing's character or standing.

C. Trust Management Systems

It has three main categories.The trust management system in the first category has a central authority, which is usually called the trust values assigned by the TTP. In the second category,one global trust value is drawn and published for each node,based on the nodes opinions toward it.The third category includes the trust management systems that allow each node to have its own view of other nodes. Many recent reputation systems such as CONFIDANT [5], CORE[6],and OCEAN[7] belong to this category. In the improved CONFIDANT [8], buchegger and boudec provided a modified Bayesian approach for reputation representation.But this approach leaves an false accusation attacks and no constraint on update frequency and lacks the ability to separate newcomers from misbehavers.

III. Security and trust

Trust and reputation systems as soft security mechanisms The purpose of security mechanisms is to provide protection against malicious parties. 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.

A. 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.

B. Communication security and trust

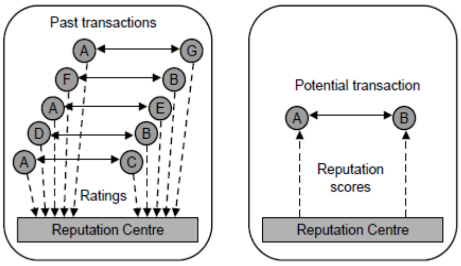
Communication security includes encryption of the communication channel and cryptographic authentication of identities.

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. *Centralized reputation systems*

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.

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 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.



a) Past b) Present

Fig.1. General framework for a centralized reputation system

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.

V. The reactive algorithm

History-based scheme is based on the random movement model, while the cross and metropolis schemes need to control ambassadors movement. Each produces different probabilities of getting authentication for the incoming nodes.

The nodes movement is not always purely random, and the destination of an outgoing node could be vague before moving. If the destinations of outgoing nodes follow certain probability distribution, a history-based dispatching scheme is useful. Using this model as the underlying mobility scheme, the outgoing node i has the probability pj to go to region Rj. Each region Rh also counts the incoming probability from another region Rj, which is the number of incoming nodes from Rj divided by the total number of nodes coming to the Rh.When selecting ambassadors, a selection period is applied. The CH will first record all the nodes that applied to move in the selection period. The CH will determine the movement until the end of the selection period. Algorithm is then applied to select k nodes to be the ambassadors. The history-based scheme shares the same ambassador seeking and visa issuing rules as the simple scheme.

Algorithm . History-based selection

```
1: while the selection period timer lasts do
2: if a node satisfies requirements and requests to move then
3: Add possible destination regions into set D, and the node into ambassador candidate set C;
4: end if;
5: end while;
6: Sort D based on $q_{j\,h}$;
7: Keep the first k regions in D and cut-off other regions;
8: for the region $R_j$ with largest $q_{j\,h}$ in D do
9: Assign CK to the node i with largest $p_{j,i}$, and announce i as the ambassador;
10: Delete $R_j$ from D and i from C;
11: end for;
```

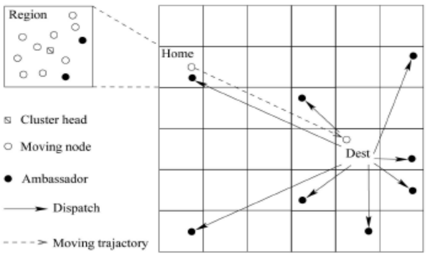


Fig2.General dispatching

A. Cross-Dispatching Scheme

In the history bases scheme, incoming nodes can be directly authenticated by an ambassador with certain probability. When the number of ambassadors is much smaller than the number of regions, the probability can be fairly low. In the cross-dispatching scheme, incoming nodes are guaranteed to be authenticated by an ambassador of the destination region. However, in this scheme, the movements of the ambassadors are not random, and indirect authentication should be allowed. Assume that regions, as shown in Fig.3..Each region sends one ambassador for each region in the same column and one ambassador for each region in the same row. For a moving node, there are two regions called joint regions in the network that have ambassadors from both its home region and destination region. Therefore, a trust transition chain an be formed if we require the moving nodes to move to a joint region before entering the destination region.

In the ambassador seeking phase, the moving node still searches its home region first. If it cannot find the ambassador of the destination region, it moves to the closest joint region to continue the searching. When a moving node cannot find an ambassador for the destination region in its home region, it turns to ask the CH to issue a visa that is verifiable to the ambassador of the home region. This visa is signed by the same cachet key as the ambassador's. When the moving node i enters the joint region, it presents its visa to the ambassador of its home region.

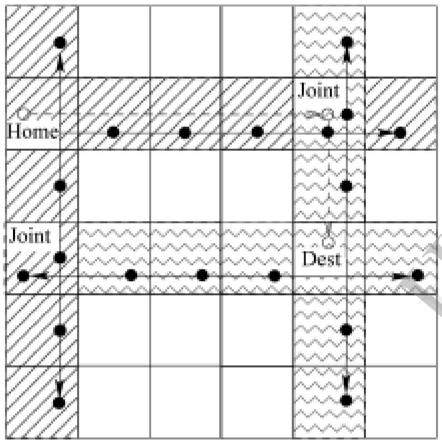


Fig.3.Cross dispatching

B. Metropolis Scheme

To offer more flexibility, a hierarchical dispatching scheme is developed. We can organize regions into areas, as shown Fig.4

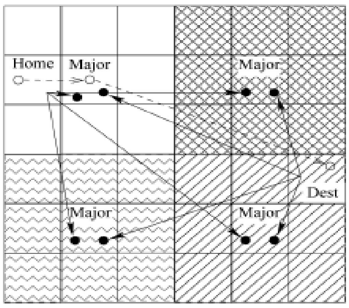


Fig4.Metropolis dispatching

In each area, a "major" region is selected. When a region decides to dispatch ambassadors, it will first send ambassadors to major regions. When a node decides to move, it obtains a visa that is verifiable to the ambassador of its home region. It then moves to the nearest major region. As the ambassador of the home region and the destination region can be found in the same "major" region, the reputation (discounted by the trust between two ambassadors) of the moving node can be passed, and it will get a visa verifiable for the destination region. The metropolis scheme shares similar ambassador seeking and visa issuing rules with the cross-dispatching scheme. The only difference is that it uses the closest major region instead of the joint region.

VI. 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

A .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 Fig 4. 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.

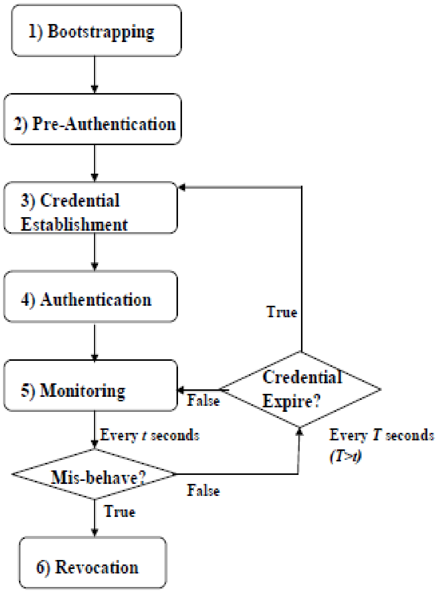
3) Credential establishment: This step establishes the supplicant's new credentials, which the system will use as proof of its identity and as a verification of its authorized state thereafter. A credential could

be a symmetric key, a public/private key pair, a commitment of a hash key chain, or some contextual information.

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.

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

B. Lightweight Integrated Authentication(LIA)

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.

C.PKI-based Integrated Authentication (PIA):

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.

VIII. Experimental analysis

History based scheme with authentication methods are implemented with the use of visual studio 2008, ASP.net,c# and SQL server 2005 as the backend. That can offer flexibility for users to achieve application specific goals.

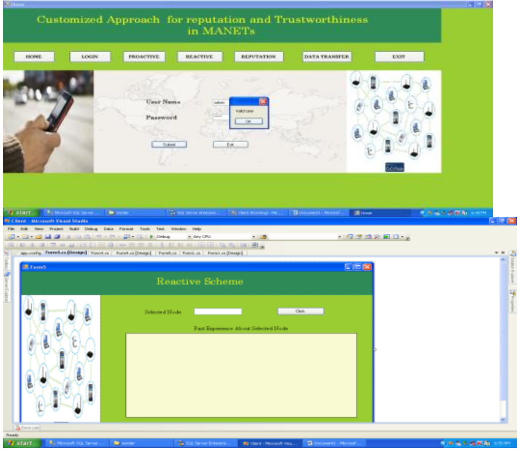


Fig5Experimental analysis

IX Conclusion

In this paper uncertainty can be reduced by, with the use of dispatching with strong authentication scheme. Mobile no des are strongly authenticated .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 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.

[11] Helen Tang, Mazda Salmanian and Connie Chang "Strong Authentication for Tactical Mobile Ad Hoc Networks"Defence R&D Canada, Ottawa technical memorandum, July 2007.

[12] 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.