AUTHENTICATION VIA AMBASSADORS: A NOVEL AUTHENTICATION MECHANISM IN MANETS

Feng Li and Jie Wu
Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL 33431

ABSTRACT

The reputation bootstrap problem is a significant issue for mobile ad-hoc networks (MANETs). We present a novel mechanism, Authentication Via Ambassadors, which authenticates mobile nodes based on their "social relationship". One commonly-trusted node is elected as the cluster head in each region. Ambassadors, which are moving nodes trusted by the cluster head, are selected and dispatched according to several different criteria to represent the region and perform authentication. A node that anticipates moving into a remote region can search and find an ambassador of that region, and take authentication to obtain a more precise initial reputation in the remote region. Therefore, the trust convergence time is reduced, and many attacks that threat the reputation systems for MANETs are avoided.

Keywords: *Authentication, reputation bootstrap, vouching.*

I. INTRODUCTION

Many reputation systems are developed for MANETs to stimulate cooperation and mitigate nodes' selfish misbehavior. Due to the unique operational environment of MANETs where nodes are allowed to move freely, the challenges for reputation systems manifest in new forms. Most existing reputation systems are constructed on the basis of nodes' communication experience. Therefore, these systems require sufficient time to form stable opinions. Since nodes' communication range is restricted, they can only communicate and monitor other nodes in a certain range. After completing their tasks in one region, they move into another region to conduct other tasks and need to buildup reputation again. This reputation bootstrap problem for mobile nodes seriously degrades the efficiency of the reputation system, increases the average uncertainty, and facilitates many attacks.

This work was supported in part by NSF grants CNS 0422762, CNS 0434533, CNS 0531410, and CNS 0626240. Correspondence email: fli4@fau.edu.

One possible mitigation mechanism for this problem is through authentication. With the ability to obtain a move-in node's reputation in its home region and authenticate that node's identity, the remote region can assign a more precise initial reputation value for the node. However, since no predefined trust exists, a novel authentication method needs to be developed to counter this problem.

User authentication in computing systems traditionally depends on three factors: something you have (e.g., a hardware token), something you are (e.g., a fingerprint), and something you know (e.g., a password). In [1], Brainard et al. explores a fourth factor: the social network (somebody you know). We extend this idea and use the fourth factor in the authentication mechanism.

When a node is expected to move into another region (called the destination region) to perform a new task, it searches its local area and tries to find the *ambassador* which moves from and represents the destination region. If such an ambassador exists in the node's social network, a recommendation, which is called a *visa* in this paper, will be issued which includes the node's current reputation and a signature verifiable to the destination region. We call this process: **A**uthentication **V**ia **A**mbassadors (**AVA**). The authentication is optional. When a node cannot find such an ambassador, it is still allowed to move but needs to endure a longer reputation bootstrap period in the destination region.

In summary, our contributions are as follows: 1) We propose the idea of the AVA by exploring the social network of mobile nodes. 2) We devise novel schemes to select ambassadors among moving nodes and dispatch them according to different criteria in order to increase the authentication probability. 3) We present supporting steps, including key distribution, ambassador seeking and visa issuing, to secure the authentication process. 4) We validate the applicability of the proposed schemes through extensive analysis and simulation.

II. RELATED WORK

Many trust management systems, such as CONFIDANT [2], CORE [3] and OCEAN [4], have been developed to

stimulate node cooperation in MANETs. Most of them allow each node to build its own trust view based on the observations as well as the recommendations from others. However, [5] presents the reputation bootstrap problem as an important issue for these systems. The long bootstrap period for the newcomer is considered to be burdensome and dangerous. When mobility is fully considered as in [6] and [7], these problems become even more severe as the topology in each region is always changing. A method to realize reputation carry-on between regions and mitigate the newcomer problem is important for the implementation of these reputations in MANETs.

In [1], Brainard et al. introduces the concept of vouching as a tool for on-line authentication. Vouching directly leverages human relationships, and this work can be seen as part of a broad exploration of the interplay between social networks and user authentication. We extend the fourth factor authentication mechanism. In our scheme, the moving node tries to find someone it knows in order to get authenticated and obtain a corresponding certificate.

In [8] and [9], uncertainty is defined and considered to be an important metric for the reputation system. In MANETs, nodes collect information through direct communication in a distributed manner and form trust opinions based on direct observations and recommendations of others. The uncertainty is unavoidable, as inaccuracy and incompleteness always exists in the collected information. Uncertainty is also the fundamental reason for the reputation bootstrap problem. Without AVA authentication schemes, nodes in the destination region will have no knowledge about the incoming node. Therefore, the uncertainty is high.

III. Design

In the model, a node stays in its home region for a long period of time before it moves. After completing the tasks in that region, the node moves to the destination region in order to conduct a new task, which usually requires a long stay and cooperation from the other nodes in the destination region. After finishing it, the destination region becomes the new home region for the node's later movement.

A. Key Distribution

As there is no infrastructure in MANETs, it is hard to find a trusted third party and use the PKI to realize authentication. In our model, each node i generates a private key RK_i and public key PK_i pair. The private key can be regarded as node i's personal secret. The public key is distributed in the home region. Nodes in the home region can use direct contact to verify the identity when it receives the public key. They also monitor the behavior of i and use a reputation system to draw trust opinions towards it.

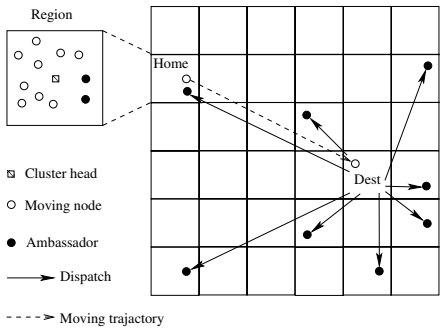


Fig. 1. Ambassador dispatching.

Some nodes are selected to act as ambassadors of their home region. For these ambassadors, their home region will assign another kind of key, called *cachet* key CK, for them. The ambassador uses CK to represent its home region and provide AVA authentication.

The CK can be implemented by using the TESLA [10] scheme. In each region, a commonly-trusted node is elected and acts as the cluster head CH in the region. It generates a keychain by recursively applying a hush function on a master key CK^1. The keychain has the form: $CK^1; CK^2 = H(CK^1)$; ...; $CK^n = H(CK^{n-1})$. Note that this keychain will be assigned reversely. When an ambassador is about to move, the CH assigned a key from the attached keychain.

B. Ambassador Dispatching

We propose four different dispatching schemes to satisfy different requirements for the outgoing nodes to be ambassadors. Each produces different probabilities of getting authentication for the incoming nodes.

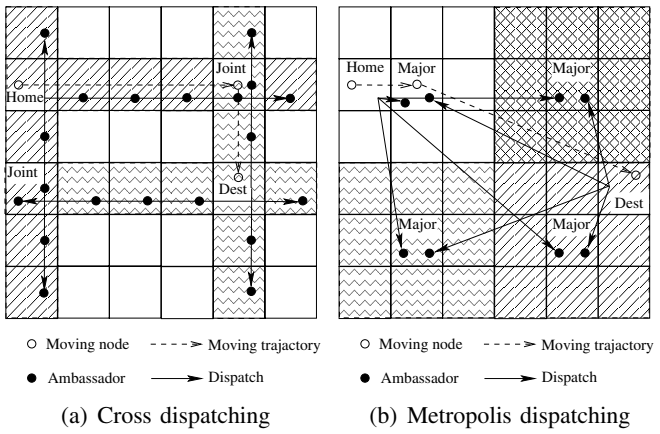
*1) **Simple selection**:* When the moving pattern for the mobile nodes complies to the random way point model, and the node knows its destination clearly, a simple selection scheme that only considers the outgoing nodes' reputation is sufficiently powerful to dispatch the ambassadors. In this scheme, 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. 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.

1) $Rep_i \geq T$.
2) The public key of i is properly stored.
3) No record indicates that an valid ambassador exists in the intended destination region of node i .

These conditions are the basic requirements for ambassadors, which are also adopted by the following schemes.

Algorithm 1 History-based selection

```
while the selection period timer lasts do
    if a node satisfies requirements and requests to move then
        Add the possible destination regions into set D;
        Add the node into ambassador candidate set C;
    end if;
end while;
Sort D based on q_h^j;
Keep the first k regions in D and cut-off other regions;
for the region R_j with largest q_h^j in D do
    Find a node i with largest p_i^j;
    Assign CK to node i;
    Announce node i as the ambassador;
    Delete R_j from D and i from C;
end for;
```



(a) Cross dispatching (b) Metropolis dispatching

Fig. 2. Dispatching Schemes.

*2) **History-based selection**:* 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. This mobility model, denoted as the restricted random way point model in [6], is considered to be more realistic.

To be formal, the outgoing node i has the probability p_i^j to go to region R_j. Each region R_h also counts the incoming probability from another region R_j, which is the number of incoming nodes from R_j divided by the total number of nodes coming to the R_h. We call this probability q_h^j.

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 deter the movement until the end of the selection period. Algo. 1 is then applied to select k nodes to be the ambassadors.

*3) **Cross dispatching**:* In the above two schemes, 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 we have $n \times n$ regions as shown in Fig. 2(a). 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 can be formed if we require the moving nodes to move to a joint region before entering the destination region. The detailed indirect authenticated method is discussed in section III-D.

*4) **Metropolis dispatching**:* To offer more flexibility, a hierarchical dispatching scheme is developed. We can organize regions into areas as in Fig. 2(b). 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 gets 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.

C. Ambassador Seeking

When a node wants to move to a region, it is better to get a visa for the destination. Consider two kinds of moving models for the node. The first is random movement, which is used in simple and history-based selection. In these two schemes, the moving node only searches its home region for an ambassador of the destination region. If it cannot find the ambassador, it directly moves to the destination.

The second is controlled movement, which should be used in the cross and metropolis dispatching schemes. The moving node still searches its home region at first. If it cannot find the ambassador of the destination region, it moves to the joint or the closest major region to continue the searching.

D. Visa Issuing

There are three possible results in the ambassador seeking phase. One is that the moving node found an ambassador of the destination region in its home region. The ambassador communicates with the CH of this region, process the authentication request, and generates a certificate as the visa. This process is illustrated in Fig. 3. In this visa, the ambassador should include node i's public key PK_i, i's

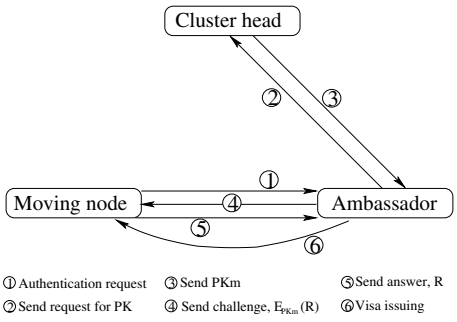


Fig. 3. Visa issuing.

reputation in the home region Rep_i, and signed by the cachet key CK from the ambassador's home region. Here, $E_{(CK)}$ means encrypting by cachet key CK.

$$visa = E_{(CK)}\{PK_i|Rep_i\} \tag{1}$$

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, broadcast the moving node's public key, and announce its reputation as the initial reputation of the moving node in the region.

In other two cases, the moving node cannot find an ambassador in its home region. Thus it has two choices: to give up visa seeking or to go along a path to get the visa for the destination region. When the cross or metropolis dispatching scheme is selected, a 2-hop visa chain is enough for the visa issuing.

In the visa issuing phase of these two schemes, 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 a cachet key in the keychain, which has a larger superscript than the ambassador's cachet key. This visa is in the form: $visa = E_{(CK)}\{PK_i|Rep_i\}$.

When the moving node i enters the joint or major region, it presents its visa to the ambassador of its home region. The ambassador verifies the signature as it has a cachet key from the keychain. The ambassador of the home region A_h then requests the public key of the ambassador of the destination region A_d from the CH of the joint or major region. The A_h sends the request for a visa to A_d, A_h's ID, and the piece of encrypt proof: $E_{(RK_{A_h})}\{E_{(PK_{A_d})}\{PK_i|Rep_i\}\}$.

After receiving the information, A_d decrypts the reputation value of the moving node, consider the value as the recommendation from A_h, and construct its opinion towards i based on Rep_i as well as its opinion towards A_h. Let Rep_i' denote A_d's discounted opinion towards i, A_d generates a new visa by using its cachet key $\tilde{CK}$ which is verifiable to the destination region: $visa' = E_{(\tilde{CK})}\{PK_i|Rep_i'\}$.

IV. Analysis

In the analysis, the following parameters are used: the network contains $n \times n$ regions; there exist m major regions when applying the metropolis scheme; each region selects k nodes as ambassadors.

A. Uncertainty Trade-Offs

Uncertainty is the most important metric which implicitly exists in the reputation bootstrap or newcomer problem. In [8], we give a formal definition for uncertainty based on the number of recorded successes α and failures β. A triplet is used to represent a node's trust opinion $(b, d, u) \in [0, 1]^3$: $b + d + u = 1$. b, d, and u designate belief, disbelief, and uncertainty, respectively.

Generally speaking, uncertainty has the following attributes. First, the greater the amount of evidence there is, the less uncertainty u there will be. Second, a recommendation always increases the uncertainty. When node i receives the recommendation $R_j^k = \{b_j^k, d_j^k, u_j^k\}$ from node j towards node k, a commonly accepted recommendation reasoning process [8] [9] is defined as follows:

$$u' = b_i^j \cdot u_j^k + d_i^j + u_i^j \tag{2}$$

$$b' = b_i^j \cdot b_j^k;\ d' = b_i^j \cdot d_j^k \tag{3}$$

where $\{b', d', u'\}$ is the resulted recommendation.

The procedure of AVA authentication can be considered a recommendation reasoning process. Using simple or history-based selection, the trust chain in this case is: 1) the ambassador authenticates and collects original reputation of the incoming node; 2) CH receives recommendation from the ambassador; 3) CH broadcasts recommendation to nodes in the destination region.

The ambassador gets moving node i's reputation from i's home region. This reputation is considered to be the base reputation with the original uncertainty. In step 2, as the ambassador is the selected delegate of CH, CH should totally trust it. In step 3, nodes discount the reputation based on their trust to the CH by applying equation 2. As the CH is the commonly-trusted node in the region, the uncertainty in the reputation should increase only a small amount.

When using the cross or metropolis dispatching scheme, the trust transition chain is more complicated: 1) the CH of the home region authenticates and collects original reputation of the moving node; 2) A_h receives the recommendation from that CH; 3) A_d receives recommendation from A_h; 4) CH of the destination region receives recommendation from A_d; 5) CH broadcasts recommendation to nodes in the destination region.

In this case, one more recommendation with reputation discount exists. Since A_h and A_d are selected by their CH

respectively before they move into the joint or major region, high disbelief or uncertainty may exist in their relationship. Applying equation 2, step 3 brings much higher uncertainty compared to the previous case.

However, there is still one more case to be examined. When a node cannot find an ambassador and moves to the destination region without getting authentication, the node will start with $u = 1$ in the new region, as the destination region has no information about the newcomer.

B. Cost Trade-Offs

The analysis of the cost focuses primarily on the number of ambassadors, and the movement model. If the cost is not considered, an extreme solution, in which each region sends ambassadors to cover all the other regions, will outperform the proposed schemes. However, it incurs a huge cost as the total number of ambassadors is $n^2 \cdot (n^2 - 1)$. Therefore, a parameter k, which is the designed number of ambassadors, can be used to achieve trade-off between cost and authentication probability in the proposed schemes.

The ambassadors' movement model is also greatly related to the cost. For schemes like simple selection and the history-based scheme, to be an ambassador is only a "part-time" job. The costs for these schemes are relatively low.

The cross scheme requires the controlled movement of its ambassadors. The number of ambassadors is fixed as $2 \cdot n$. Its cost is relatively high compared to other schemes, but that is necessary to achieve the guaranteed authentication. If the region diameter is regarded as the unit distance, the total additional moving distance is:

$$2 \cdot n \cdot (\sum_{i=1}^{n}((i-1) \cdot i) + (n-i) \cdot (n-1+1)) = O(n^4) \quad (4)$$

The metropolis scheme is the most flexible one to achieve the cost trade-off. When the $k < m$, the cost and successful authentication trade-off can be achieved by adjusting k. When $k = m$, the guaranteed authentication is achieved.

C. Delay Trade-Offs

We use relative moving delay, which is the time a moving node takes to find the ambassador, get authenticated, and move to the destination region compared to the time that the moving node needs to directly get to the destination region. For the simple or history-based selection scheme, the relative moving delay is 1, as the moving node will not change its trajectory to find an ambassador.

For the cross and metropolis schemes, the relative moving delay for the cross scheme varies from 1 to $\sqrt{2}$. The best case is the home and the destination region are in the same column or the same row. The relative moving delay of the metropolis scheme depends on the number of predefined major regions m. If the major regions are uniformly distributed in the network, larger m will lead to smaller relative moving delays. In this scheme, the worst case occurs when the home and destination region are adjacent to each other while their distance to the closest major region is the maximum possible value. Therefore, the worst relative moving delay is $2\sqrt{2} \cdot \sqrt{\frac{n^2}{m}}$.

D. Authentication Probability

The probability of successfully getting authenticated depends on the parameter k. For the simple selection scheme, this probability is quite direct. As each region randomly selects ambassadors for k other regions, the authentication probability is $\frac{k}{n^2-1}$.

For the history-based scheme, a region R_h records the history sources of the incoming nodes and ranks these source regions according to the incoming probability q_h^j. The outgoing nodes with higher probability to go to those higher ranking regions will have higher priority to be selected as the ambassador. Suppose the first k ranked source regions are R_1, ..., R_k, and the incoming probability is q_h^1, ..., q_h^k. The probability that a incoming node comes from the rest of the n^2-k-1 regions is $q = 1-q_h^1-...-q_h^k$. The authentication probability in this case is:

$$\sum_{j=1}^{k}(p_i^j \cdot q_h^j) + \frac{\sum_{j=1}^{k}((1-p_i^j) \cdot q)}{n^2-k-1} \quad (5)$$

This probability can be significantly higher than that for simple selection if most incoming nodes are from fewer then k regions.

The major advantage of the cross scheme is to guarantee that the moving node meets an ambassador from the destination region and gets authenticated. So, the probability of authentication is 100% in this case.

The metropolis scheme is relatively flexible. When $k \geq m$, the successful authentication probability is 100% as the moving node can always find ambassadors from its home region and the destination region in the closest major region. When $k < m$, the probability is equal to the probability that both ambassadors from the home region and the destination region existing in the closest major region, which is $(\frac{k}{m})^2$.

E. Security Analysis

Attacks, such as bad mouthing or faked identity, are considered as general problems in reputation systems. As the proposed schemes are exploited to mitigate the reputation bootstrap problem, the influence of these attacks changes.

Bad mouthing occurs where malicious parties provide dishonest recommendations of other nodes [5]. In the AVA

Table I Comparison of different schemes

Dispatching schemes	Simple selection	History-based	Cross	Metropolis
Recommendations with increasing u	1	1	2	2
Number of ambassadors	k	k	$2 \cdot n$	k
Movement scheme	Random	Random	Controlled	Random/Controlled
Moving delay	1	1	$\leq \sqrt{2}$	$\leq 2\sqrt{2} \cdot \sqrt{\frac{n^2}{m}}$
Authentication probability	$\frac{k}{n^2-1}$	$\sum_{j=1}^{k}(p_i^j \cdot q_h^j) + \frac{\sum_{j=1}^{k}((1-p_i^j)\cdot q)}{n^2-k-1}$	1	$(\frac{k}{m})^2$ when $k < m$; 1 otherwise

schemes, the destination region gives the initial reputation to the incoming node purely according to the ambassador's recommendation. If the ambassador conducts the bad mouthing attack, the initial reputation will be biased. However, the defense against this attack is three-fold: 1) The ambassadors are carefully selected by the CH. They need to have a qualified reputation in their home region before they become the ambassador. 2) The recommendations are discounted according to equation 2. 3) The CH can impose a valid period for each ambassador, which is realized by revoking keys in the keychain periodically.

If a malicious node can create several faked IDs, the reputation system suffers from the Sybil attack [11]. Mobile nodes in MANETs can conduct Sybil attacks purely by sophisticated movement. A node can behave maliciously in one region. After its reputation becomes low in that region, it will move to another region without being authenticated even when it can find an ambassador from the destination region. Its reputation will be bleached in the new region. This attack can be mitigated by forcing mobile nodes to get authentication before entering its destination region when using the cross and metropolis scheme.

V. Simulation Evaluation

We compare the following AVA schemes in the simulation: (1) Simple selection. (2) History-based selection. (3) Cross dispatching. (4) Metropolis dispatching.

A. Simulation Environment

We use a discrete event simulator for the simulation study. All protocols are evaluated in a network with both static nodes and mobile nodes randomly deployed in a $1000m \times 1000m$ area. The normal transmission range is $100m$. The area is uniformly divided into regions, and each region has 40 nodes including 30 possible mobile nodes.

Nodes actual behaviors comply to the Bernoulli trial. The uncertainty-oriented reputation system defined in our work [8] is used as the sample system. Each node monitors other nodes in the same region, and records the number of good or bad activities in α or β towards each node. All nodes remain static and build up reputations in their home region in the initialization period. The CH, which is the static node with the highest reputation, is elected in each region. When the initialization period ends, ambassadors are selected and moving nodes are allowed to move. All simulations are repeated 2000 times to get reliable results.

B. Simulation Results

In Figs. 4(a) to 4(d), the reputation threshold for the ambassador is $b \geq 0.7$ and the number of ambassadors is fixed as $k = 15$. We adjust n which decides the number of regions ($n \times n$) to compare the schemes, n varies in $[5, 15]$.

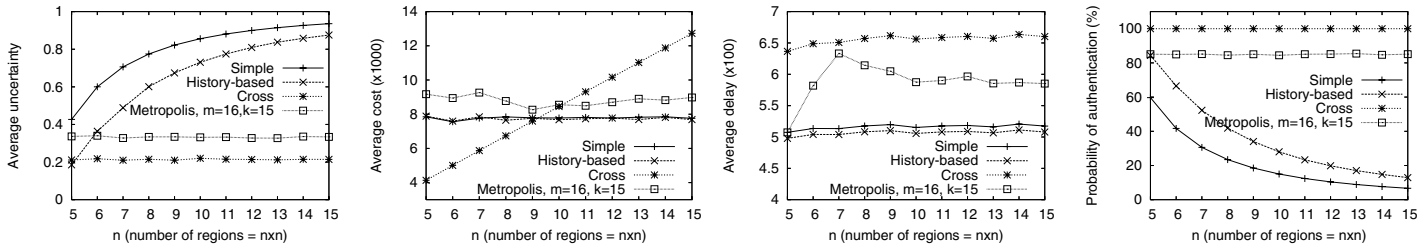
In Fig. 4(a), the uncertainty u is calculated when the moving node enters a destination region. Without AVA authentication, the uncertainty for the incoming node is $u = 1$. Since cross and metropolis schemes require two hops of general recommendations, the uncertainty increase in this process should be higher then in the authentication process of simple or history-based selection scheme. According to our simulation, the average uncertainty is 0.553 in the 2-hop recommendation, and 0.039 in the 1-hop recommendation.

However, the average uncertainty in the cross and metropolis schemes are still significantly lower. There are two reasons: 1) Ambassadors are selected by the CHs. They have qualified reputation which implies more trustworthy behavior. 2) The probability of finding the ambassador in the cross and metropolis schemes are higher.

In Fig. 4(b), the cost is defined as the total travel distance of the ambassadors from a single region. In the metropolis and cross scheme, ambassadors need to move to designated regions, which makes the cost higher. The cost in the cross scheme appears to increase linearly since the ambassadors' average moving distance remains the same and the number of ambassadors from each region is $2 \cdot n$. Comparatively, the metropolis scheme is preferable as the cost of this scheme only depends on number of major regions m.

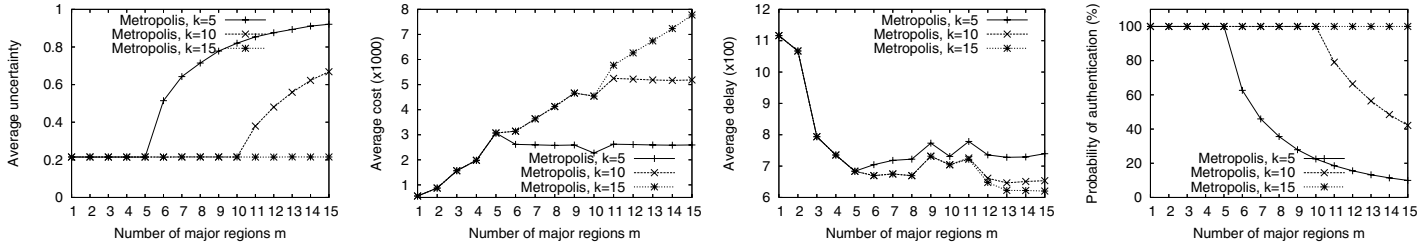
In Fig. 4(c), the speed v of moving node equals $1.0\ m/s$. 10000 source and destination pairs are randomly generated, and the sum of the moving and waiting delay are collected. The delay of the cross and metropolis schemes are higher since the moving nodes moves to the closet joint or major regions instead of directly to the destination.

In Fig. 4(d), the curves show a similar pattern as in Fig. 4(a). This implies that uncertainty mainly depends on



(a) Uncertainty (b) Cost (c) Delay (d) Authentication probability

Fig. 4. AVA authentication scheme comparison with different region size.



(a) Uncertainty (b) Cost (c) Delay (d) Authentication probability

Fig. 5. Metropolis scheme comparison with different number of major regions.

the authentication probability, when nodes actual behavior complies to the uniform distribution. The probability of authentication is much higher in the case of cross or metropolis scheme. It makes these schemes preferable in applications where additional cost and delay aren't the major concern, and lower uncertainty for newly incoming nodes is one of the main goals.

Considering the results in Fig. 4 synthetically, the metropolis scheme seems to be more flexible in terms of the trade-off among delay, cost, authentication probability, and uncertainty. Therefore, the simulations in Fig. 5 use similar settings as in Fig. 4. We then adjust m and show the results of different combinations of k and m. The number of regions is fixed at $n^2 = 100$.

The results in Fig. 5 can be summarized as: 1) Increasing m can significantly reduce delay when the number of regions $n^2 >> m$. 2) k can be adjusted to achieve fine-grain trade-off between cost, delay, and authentication probability. 3) k should be selected closer to m. Otherwise, the probability of authentication drops very fast as m increases.

VI. Conclusion

Reputation bootstrap is an important issue for these systems, especially when nodes are allowed to move freely. In this paper, an AVA mechanism that authenticates mobile nodes based on ambassador vouching is presented. Four ambassador dispatching schemes, corresponding ambassador seeking, and visa issuing schemes are presented and compared in terms of authentication probability, delay, cost and uncertainty. An extensive simulation study shows that the authentication scheme significantly decreases trust convergence times for mobile nodes. Our future work will focus on integrating the AVA authentication mechanism with an established reputation system in MANETs.

References

[1] J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Yung. Fourth factor authentication: Somebody you know. In *Proc. of CCS*, 2006.

[2] S. Buchegger and J. Boudec. Performance analysis of the confidant protocol. In *Proc. of MobiHoc*, 2002.

[3] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Communications and Multimedia Security*, pages 107–121, 2002.

[4] S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks. *CoRR*, cs.NI/0307012, 2003.

[5] S. Buchegger and J. Boudec. A robust reputation system for p2p and mobile ad-hoc networks. In *Proc. of the Second Workshop on the Economics of Peer-to-Peer Systems*, 2004.

[6] S. Capkun, J. Hubaux, and L. Buttyán. Mobility helps security in ad hoc networks. In *Proc. of MobiHoc*, 2003.

[7] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502, 2002.

[8] F. Li and J. Wu. Mobility reduces uncertainty in MANETs. In *Proc. of INFOCOM*, 2007.

[9] A. Josang. An algebra for assessing trust in certification chains. In *Proc. of NDSS*, 1999.

[10] A. Perrig, R. Canetti, J. Tygar, and D. Song. The tesla broadcast authentication protocol. *RSA CryptoBytes*, 2002.

[11] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proc. of IPSN*, 2004.