AUTHENTICATION EMPLOYING NEIGHBOR TABLES IN MOBILE AD HOC NETWORKS

Dorsaf Azzabi, Kunihito Tanaka, Ushio Yamamoto and Yoshikuni Onozato
Graduate School of Engineering, Gunma University 1-5-1 Tenjin-cho, Kiryu, Gunma, 376-8515, Japan

Keywords: MANET, transmission range, mobility, neighbor authentication.

Abstract: In this paper we investigate the authentication mechanism in mobile ad hoc networks (MANET). Developing a trustworthy authentication mechanism in a dynamic and volatile ad hoc mobile setting is a complex task. The goal of this paper is to propose an authentication mechanism to validate the existence of neighborhood in MANET. We focus on common adjacent nodes which can authenticate and trust a mobile node. Simulation results show the existence of common adjacent nodes that are able to establish trust and obtain the effective range of neighbor authentication in terms of transmission range and node density.

1 INTRODUCTION

Ad-hoc networks are based on naive "trust-your-neighbor" relationships. Such relationships originate, develop and expire on the fly and usually have short life spans. As the overall environment in such a network is cooperative by default, these trust relationships are extremely susceptible to attacks. For a number of reasons, including better service, selfishness, monetary benefits or malicious intent, some nodes can easily mould these relationships to extract desired goals. Also, the absence of fixed trust infrastructure, limited resources, ephemeral connectivity and availability, shared wireless medium and physical vulnerability, make trust establishment virtually impossible. To overcome these problems, trust has been established in ad-hoc networks using a number of assumptions including pre-configuration of nodes with secret keys, or presence of an omnipresent central trust authority

Authentication mechanisms in mobile ad hoc networks (MANET) are very important since the role of MANET is to get information through nodes by ad hoc mode in the network field. In MANET the communication among nodes to relay information is exposed to various security attacks. There have been many works for authentication. However authentication for MANET especially for moving nodes is usually left to future research. L. Lazos et al. (Lazos, 2005) describe typical security threats such as the wormhole attack and the Sybil attack. They propose the SeRLoc for the secure localization in the presence of these threats. They show, based on their performance evaluation, that it is robust against various sources of error. But they do not consider mobile nodes.

LITEWORP (Khalil, 2005) allows detection of the wormhole by isolating the malicious nodes. The detection is based on a local monitoring using neighbor lists. A node will not receive a packet from a node that is not a neighbor nor forward to a node which is not a neighbor. It is not assessed whether the LITEWORP is applicable to the mobile situations. Azzabi and Uchihara et al. (Azzabi, 2007) proposed their neighbor authentication mechanism for neighboring nodes that can cope with nodes mobility and hostile environments.

Importance of secure neighbor discovery in wireless networks is explained by Poturalski et al. (Poturalski, 2008). Time-based protocols and time- and location-based protocols to achieve secure neighborhood discovery are proposed and proved in a formal model. Their protocols are applicable even in low-density networks.

In this paper we focus on the neighbor authentication mechanism (Azzabi, 2007) utilizing neighbor tables which might be practical in ad hoc mobile environments, since developing a trustworthy authentication mechanism in a dynamic and volatile ad hoc mobile setting is a complex task. We will demonstrate the proposed neighbor authentication mechanism in this paper operate in such hostile environment. The goal of this paper is to extend effective range of the neighbor

Azzabi D., Tanaka K., Yamamoto U. and Onozato Y. (2008).
AUTHENTICATION EMPLOYING NEIGHBOR TABLES IN MOBILE AD HOC NETWORKS.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 47-52
DOI: 10.5220/0002027300470052

authentication mechanism in MANET. We investigate how to increase common adjacent nodes which can authenticate and trust a mobile node. Simulation results show the existence of common adjacent nodes that are able to establish trust and obtain the effective range of neighbor authentication in terms of transmission range and node density.

2 NEIGHBOR AUTHENTICATION MECHANISM

2.1 Network Model

We assume a MANET shown in Fig.1 where mobile nodes are randomly allocated and move according to the random waypoint model (Bettstetter, 2004) where the length of each leg is limited within a mobility range *M*. Transmission range of each node is fixed as *r*. Packets are transmitted through nodes in an ad hoc mode. All packets are gathered at the Base Station (BS). The network topology changes dynamically since the nodes are mobile.

All mobile nodes *NN* in the MANET have two kinds of their neighborhood tables: Physical existence table (P-table) and Authentication table (A-table). P-table lists all nodes within the transmission range of the node. A-table lists all authenticated nodes within the transmission range of the node. Furthermore a mobile node constructs Enlarged authentication table (E-table) based on the A-table. E-table shows all authenticated nodes of the node and its authenticated nodes within the transmission range of the node. Therefore E-table is constructed by combining A-table of the node and the ones of the authenticated nodes. When a node moves, the neighborhood tables are updated. A received packet is authenticated based on the node which has sent it. A node does not receive a packet from a node that is un-authenticated nor forward to a node which is not a neighbor (Khalil, 2005). Any node in the neighborhood tables has to be authenticated in order to keep a secure communication. That is why, for a malicious node to attack the MANET, its only opportunity is to enter in the neighborhood table.

Nodes in a MANET are classified as the following three nodes: authenticated nodes, unapproved nodes and isolated nodes. Authenticated nodes have been recognized in the network by their neighborhood relationships. Unapproved nodes are not approved by the neighbor authentication mechanism. Isolated nodes have not been in communication with other nodes.

We assume that all nodes initially distributed are not malicious nodes. We investigate authentication mechanism for new comers after initial settings so that we can keep secure communications for mobile nodes in hostile environments.

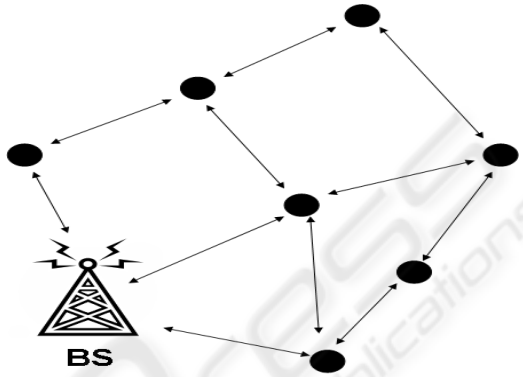

Figure 1: A MANET where packets are transmitted through nodes in an ad hoc mode. All packets are gathered at the BS.

2.2 Neighbor Authentication Mechanism for MANET

In order to authenticate a node, it is necessary to check the existence of common adjacent nodes and examine all nodes within its transmission range. This authentication process is executed employing two neighborhood tables; P- and A-tables, and enlarged authentication table E-table. Theses tables are initially constructed when all nodes are allocated at initial position. In this process, P-table is constructed at first by exchanging beacon including the node ID. Then, each node copies its own P-table to A-table, because all nodes are initially reliable by our assumption. Next, the node asks all nodes in its A-table to reply its A-table. Combining all received A-tables, the node construct E-table.

When a node moves into the transmission range of another node, three tables need to be updated. Especially, updating A-table needs the existence of common adjacent nodes. Common adjacent nodes only can authenticate newly detected node.

The authentication mechanism is explained in Fig.2. Assume the two nodes n_x and n_y where n_y is moving into the transmission range of n_x as shown in Fig.2. We explain how n_y constructs three tables: P-, A- and E-tables. Both n_x and the neighboring nodes of n_y always monitor the way n_y behaves. They may only give the authenticity of n_y. When n_y moves, there are two common adjacent nodes of n_x and n_y,

i.e. n_1 and n_2 as shown in Fig.2. They mediate between n_x and n_y. n_x searches E-table and finds that n_1 and n_2 are common adjacent nodes, namely, they authenticates both n_x and n_y.

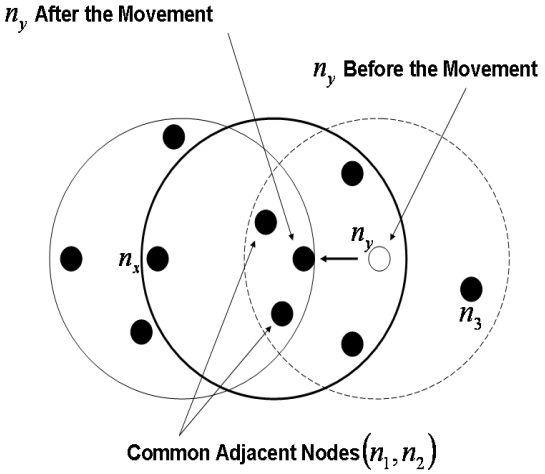

Figure 2: Common adjacent nodes after the movement of n_y.

The authentication algorithm is given as follows:

Step1) n_y (moving node) broadcasts a randomly generated nonce value (Lazos, 2005).

Step2) n_x receiving the broadcast from n_y responds with the ID of n_x and the received nonce value.

Step3) n_y realizes that it is entering the transmission region of n_x. And n_y searches for the common adjacent nodes from E-table. If the common adjacent node exists, n_y asks a confirmation of authenticating n_x to the common adjacent nodes. In this case, n_x also asks a confirmation of authenticating n_y to the common adjacent nodes. When the common adjacent node receives confirmation packets from both n_y and n_x, it recognizes that they are justified nodes, then it replies to them. After receiving this reply, n_y appends n_x to the A-table. If n_y can't receive such reply, it does not add n_x to the A-table.

Step4) n_y asks all nodes in its A-Table to send back their A-tables to ny.

Step5) After receiving all A-tables, n_y construct E-table by combining all A-tables so far received.

In order to extend effective range of the neighbor authentication mechanism, in Step 4) in the above algorithm, we enlarge asking range of n_y to neighbors of authenticated nodes, which we call one-step neighbors. Furthermore we enlarge asking range of n_y to one by next neighbors, which we call two-step neighbors. When authenticated nodes are sparsely located, this extension of authentication does not increase authenticated nodes so much. However in rather dense node distributions, we will show the effect of the extension in the next section.

We also introduce the following two control messages to isolate the malicious nodes when we detect attacks such as the wormhole: *an accusation message* and *a suspicion message* (Azzabi, 2007).

The accusation message is sent to the BS when a node finds a malicious node in the neighborhood list. BS deletes the malicious node if BS receives a number of accusation messages beyond the threshold. The suspicion message is sent to the BS when a node doubts the neighborhood relationship. BS asks, in that case, all nodes to delete the suspicious node from their neighborhood lists.

In order to detect the malicious node with the collaborative detection in the above mechanism, common adjacent nodes are necessary so that authenticity of the node is verified. We take in consideration the condition that nodes are not isolated in mobile situations, where the proposed authentication mechanism works and the trust is placed.

2.3 Countermeasure Against Malicious Nodes

In this paper we assume that all nodes initially distributed do not include any malicious node so that all neighbor tables are correct at the initial state. We investigate authentication mechanism works sound for updating in case when any malicious nodes attack after initial settings we can keep secure communications for mobile nodes in hostile environments.

If one malicious node attacks by forging P-table, or A-table, the above mechanism can detect illegal updating of the tables. Even though unjustly fabricated authentication node can be detected by legitimate nodes. When two malicious nodes attack, if we can separate the two compromised nodes, the above mechanism can detect. However if the two nodes are in proximity or collude with such as in a wormhole link, we cannot detect them (Tanaka, 2008). This is left for future research.

We will describe more about these control mechanisms in our future work. So far, the scope of this paper is to verify via simulation the idea of neighbor authentication, that is if a neighbor exists or not, because it is a fundamental prerequisite, in order to implement the before mentioned trust control messages.

3 SIMULATION SCENARIO AND RESULTS

3.1 Simulation Scenario

We consider simulating, as mentioned above, the authentication mechanism of adjacent nodes. The proposed authentication mechanism needs cooperation and coordination scenarios in ad hoc mobile environments so that isolated nodes should not be left so. We consider authenticated nodes as the nodes that have been recognized in the network by their neighborhood relationships. Isolated nodes are the nodes that have not been in communication with other nodes. Unapproved nodes are defined as nodes which are not authenticated by any node within its transmission range even though there are nodes within its transmission range. The number of isolated nodes and the number of unapproved nodes are indeed important parameters to evaluate the performance of the neighbor authentication mechanism.

We randomly distributed *NN* nodes within 100x100 rectangular area where we set *NN*=100, 200, 300, 400, and 500, and the transmission range *r*= 1, 2, 3, …, 9. We assume that each node moves according to the random waypoint model (Bettstetter, 2004) within a mobility range *M* for each movement, where *M*= 1, 2, 3, …, 9. We measure the number of authenticated nodes, the number of isolated nodes, and the number of unapproved nodes.

3.2 Simulation Results

The percentage of authenticated nodes among *NN* nodes for various values of mobility range when *r*=9 is shown in Fig. 3. As *NN* increases, the numbers of authenticated nodes increase. When mobility range is much higher, the percentage of authenticated nodes is very low. It is very understandable that if the nodes are very mobile, the communication environment is not stable unless the transmission range is set proportionally to cope with the high mobility rate. This is shown through the slice authentication distribution improvement when *r*=9.

The percentage of isolated nodes for various values of mobility range is shown in Fig. 4. As *NN* increases, the numbers of isolated nodes decrease when mobility range is much smaller. In Figs. 5 and 6, we notice that from a transmission range from 1 to 9 the number of isolated nodes tends to decrease for various mobility ranges varying between 1 and 9. The percentage of isolated nodes decreases as *NN* increases. The bigger the number of nodes is and the larger the transmission range is, the more common adjacent nodes are kept in the network where a node is not fixed in one position.

The numbers of unapproved nodes for various values of mobility range are shown in Figs.7 and 8. As *r* increases, the number of unapproved nodes increases until the neighbor authentication mechanism works. In Fig.7, as *NN*=100, the number of unapproved nodes increases especially for a higher mobility range (from 2 and above) because the nodes can cover more transmission areas so that chances of authentication occurs but failed. However when the number of nodes is much higher as shown in Fig. 8, where *NN*=500, the number of unapproved nodes decreases for increasing transmission ranges. This is because of the authentication mechanism the number of unapproved nodes decreases. In Fig. 8, all curves seem to have the similar tendency.

In Fig. 9, isolated, authenticated and unapproved nodes for the cases of one-step neighbor and two-step neighbor are depicted in the four sections where LEFTUP shows position of nodes, RIGHTUP shows one-step neighbor case, RIGHTDOWN shows two-step neighbor case, and LEFTDOWN shows augmented relations because of increased authentication process where *NN*=500, *r*=10 and *M*=9. There are 358 authenticated nodes. In the one-step neighbor case, 101 authenticated nodes increase because of enlarging to one-step neighbor. There are still 41 unapproved nodes.

Our algorithm checks for and confirms the idea that a node is authenticated by its neighbor. Our graphs show two main parameters in this simulation that influence the authentication process: node mobility and transmission range. The higher the transmission range is, the better the percentage of authenticated nodes is. When node density increases, and the transmission range increases, the trust increases. The parameters in form of authentication percentage and isolated nodes ratio indicate the performance measures.

So far we have been simulating the first aspect of our algorithm. Using the neighborhood table, if a node has a neighbor, it is authenticated, if it has not, it is not. We conclude that only neighboring nodes can authenticate an existent node. We tested the neighbor authentication method to determine under which parameters it works (the region, the transmission range etc.). We verified it for a different range of nodes mobility and transmission rage.

4 CONCLUSIONS

We simulated an authentication mechanism for establishing trust in MANET. Our aim is to investigate and describe the fundamentals behind nodes interaction while considering their mobility range with different transmission ranges. As common adjacent nodes increase, more nodes are authenticated under the proposed mechanism. Through our simulation study we show in which cases the authentication is achievable so that we could in a next level introduce the trust control messages (accusation message and suspicion message) in order to establish a trust relationship among the neighboring nodes.

This level will be explored in our upcoming paper. We will try to simulate the impact of these messages on the behavior of the MANET. We also, ought to mention that the interference problems associated with the large number of nodes as well as hidden terminal problems with enlarged transmission ranges have to be reviewed in our future study.

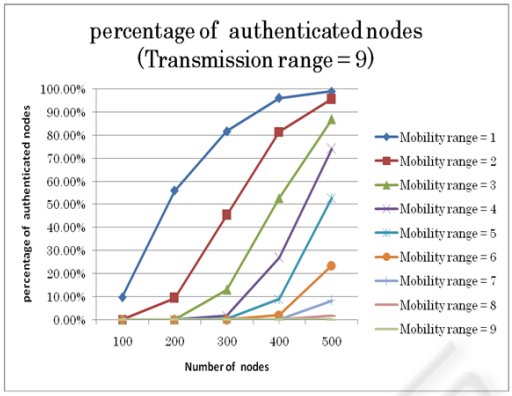

Figure 3: Percentage of authenticated nodes for various values of mobility range when r=9.

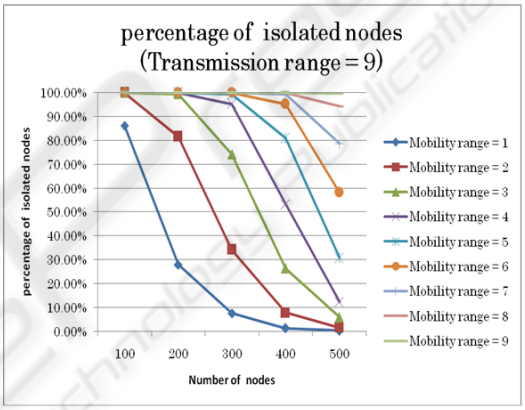

Figure 4: Percentage of isolated nodes for various values of mobility range when r=9.

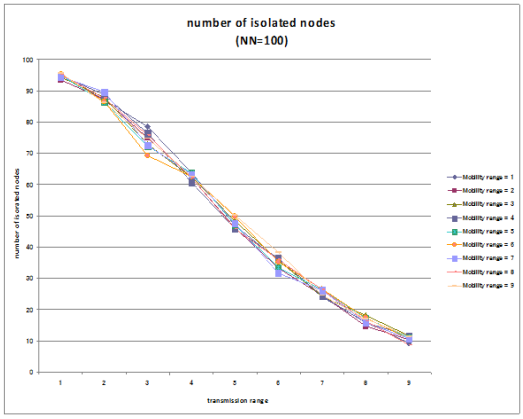

Figure 5: Number of isolated nodes versus transmission range for various values of mobility range with NN = 100.

REFERENCES

Lazos, L., Poovendran, R., 2005. SeRLoc: Robust localization for wireless sensor networks, *ACM Transactions on Sensor Networks*, vol.1, no.1, pp.73-100.

Khalil, I., Bagchi, S., Shroff, N.B., 2005. LITEWORP: A lightweight countermeasure for the wormhole attack in multi-hop wireless networks, In *the International Conference on Dependable Systems and Networks (DSN)*, pp.612-621.

Azzabi, D., Uchihara, N., Tanaka, K., Onozato, Y., 2007. Simulation of authentication mechanism in MANET, In *The Second Asia-Pacific Symposium on Queueing Theory and Network Applications (QTNA)*, pp.289-296.

Bettstetter, C., Hartenstein, H., Perez-costa, X., 2004. Stochastic properties of the random waypoint mobility model, *Wireless Networks*, vol.10, pp.555-567.

Poturalski, M., Papadimtratos, P., Hubaux, J.P., 2008. Secure neighbor discovery in wireless networks: Formal investigation of possibility, In *ASIACCS'08*, pp.189-200.

Tanaka, K., Onozato, Y., 2008., Node management method using authentication process with neighbor table in ad hoc network, *IPSJ SIG Technical Report*, 2008-MBL-44, pp.237-244.

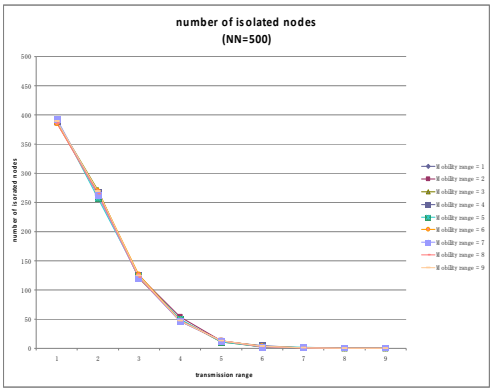

Figure 6: Number of isolated nodes versus transmission range for various values of mobility range with NN = 500.

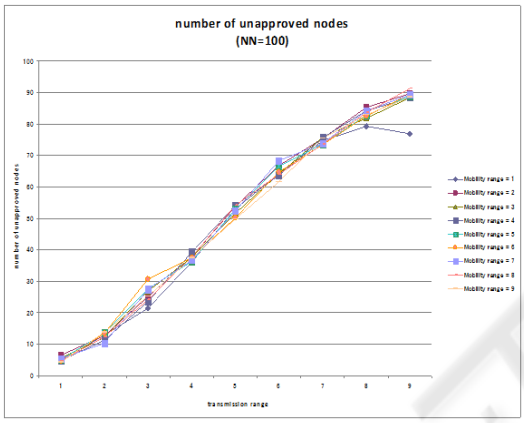

Figure 7: Number of unapproved nodes versus transmission range for various values of mobility range with NN = 100.

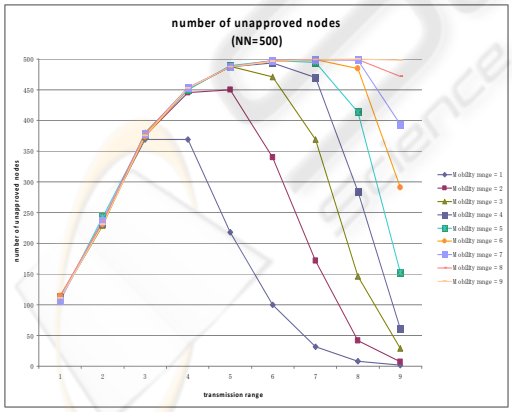

Figure 8: Number of unapproved nodes versus transmission range for various values of mobility range with NN = 500.

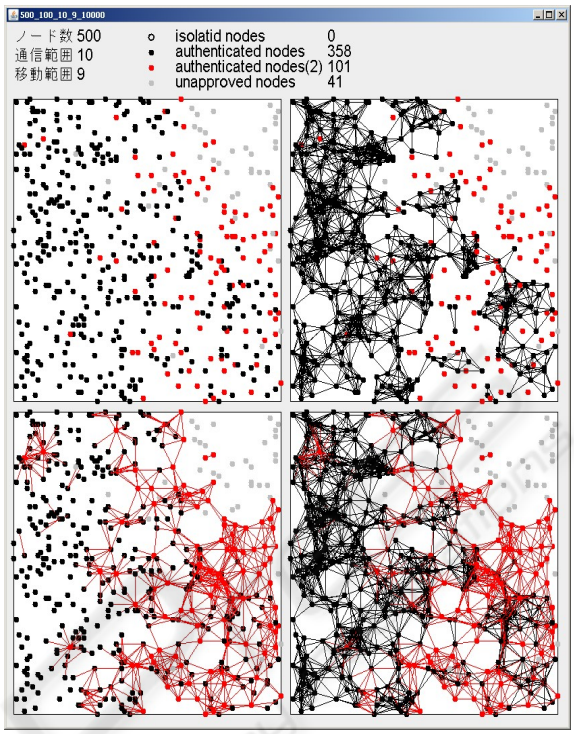

Figure 9: Isolated, authenticated and unapproved nodes for increasing authenticated nodes are depicted in the four sections where LEFTUP shows position of nodes, RIGHTUP shows one-step authentication process, RIGHTDOWN shows two-step authentication process, and LEFTDOWN shows augmented relations because of increased authentication process(NN=500, r=10, M=9).