Multi-layer Location Verification System in MANETs

Jingyi Dong(✉)

School of Electrical Engineering and Telecommunications,
The University of New South Wales, Sydney, Australia
jennied_jiyue@163.com

Abstract. The mobility and feasibility of mobile ad hoc networks (MANETs) have to deeply rely on the accurate location information to support multiple applications. A wrong announced location of a node may cause some serious consequences. Thus, the localization and the location security should be considered as important parts of the whole design of the MANETs. In the traditional way, the location verification schemes need complex calculation and multi-step communication with base stations and other vehicles, which are strengthen the burden of the MANETs routings and increased the complexity of protocol. In this paper, an improved multi-layer location verification system (MLVS) based on the optimal common neighbor's knowledge between claimer and verifier in MANETs is been proposed and discussed. In this system, each node in MANETs could have a trust value, and a mutually shared token scheme is provided to make the decision of the MLVS. Furthermore, the MLVS shows a reliable performance on the ability of attacker defense and accuracy in high node density networks.

Keywords: Mobile ad hoc networks · Location verification system · MLVS · Location security

1 Introduction

As several innovative technologies of multi-hop ad networks, the mobile ad hoc networks (MANETs), it has been one of the most popular and interesting topics for researchers. The major characteristic of MANETs is that many mobile terminals and low-cost sensors are consisted, and the packets are delivered between wireless interfaces following the geographic routing. To achieve a better performance and support possible applications, some localization schemes should be deployed into sensors and terminals, such as Global Positioning Systems (GPS). However, the openness and public ability of the wireless communication makes that the localization of MANETs could be easily attacked by malicious nodes [1]. Hence, the accuracy of the location information plays a significant role to protect the sensors' privacy, and the way to authenticate location information has been concerned [2–6]. Figure 1 illustrates the basic concept of location verification.

Q. Liang et al. (eds.), *Communications, Signal Processing, and Systems*, Lecture Notes in Electrical Engineering 516,
https://doi.org/10.1007/978-981-13-6504-1_169

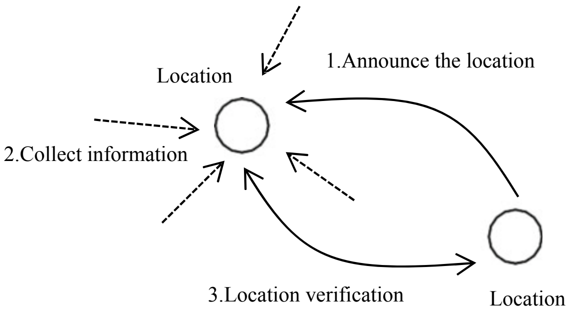

Fig. 1. Basic concept of location verification

A basic binary rule is proposed for location verification system between claimer and verifier in [7]. However, some measurements are difficult to acquire without line-of-sight (LOS). Therefore, the cooperative nodes' location communication scheme is proposed with the protocol and routing techniques' help [8, 9]. Compared to the other routing techniques, geographic routing has got foremost attention for information transmission in vehicular communication [10–12], and the information of neighbors can be obtained [13].

In this paper, a two-layer location verification system with neighbors' knowledge in mobile ad hoc networks is proposed; it follows the basic principle of mutually shared region-based location verification (MSRLV) in WSNs [14]. In layer one, LVS would roughly eliminate some malicious nodes and create a trust value table for nodes. Then, in layer two, the trust weight of common neighbors would be signed as the preparation to create a mutually shared model; the selected common neighbors in shared region between verifier and claimant provide the common knowledge to both verifier and claimant. With the information collected from neighbors, the system shows a good performance with higher node density. However, the location error would be increased in sparse MANETs.

2 System Model

In this section, some assumptions are considered for the network as follows: The mobile terminals and sensors have the same wireless transmission range r; assume that the network contains N nodes. Some of them are malicious nodes n_m, which may provide a fake location to others. The nodes' location is assumed to be obtained by GPS which is considered as the true location neglecting the localization error; we assume that the node (source) who sends the data first is not a malicious node, and following the protocol, the hops between source and destination must do the location verification before the data transmission.

The transmitted data of nodes is $n_i\{\text{data}_i, L_i, \text{RV}_i\}$, where data_i is the data transmitted by the node n_i, L_i is the announced location, and RV_i is a random value which would be discussed in next section.

2.1 Layer 1: Trust Value Table (TV)

The trust value table (TV) is constructed by several factors which are RSSI, moving direction and relative speed.

The RSSI is capable of roughly eliminating some malicious nodes who provide fake locations. The node n could obtain the received signal power $P^r_{n_j}$ from its one-hop neighbors n_j to measure the distance d_{n_j} using RSSI. At the same time, the $P^r_{n_j^*}$ could be calculated with announced location from n_j with $d_{n_j^*}$. In ideal state, the malicious node could pass the estimation only if $d_{n_j} = d_{n_j^*}$. However, considering the mobility of the MANETs, some error may be caused by complex wireless environment. In this term, a filter could be proposed to eliminate some malicious points with the threshold α; the neighbors who pass the distance filter can consist into a set S_{neighbor} with their different level.

$$\beta_i = 1 - \left| P^r_{n_j} - P^r_{n_j^*} \right| / P^r_{n_j^*} \tag{1}$$

where β_i is the i-th neighbor's distance different level of n_i. The β_i would be stored in $S_{\text{neighbor}}\left\{ n, \beta_n; \left| P^r_{n_j} - P^r_{n_j^*} \right| < \alpha \right\}$. However, the RSSI could only eliminate some malicious nodes which fake their location with a large distance difference; in some cases, the system may be suffered from the similar distance-based malicious node (SDM attack). Hence, a mutually shared region token scheme (MSR) is considered to deploy as layer two of the LVS [14]. To achieve a better performance, a trust value is regarded as the standard about common neighbors' selection in layer two. The probability that the neighbors passed the distance filtering, the relative speed and the relative distance between verifier and claimant are the factors contributing to the trust value. The model of the network is shown in Fig. 2, the node n could be seen as the verifier n_v, and the next-hop node could be seen as the claimant n_c.

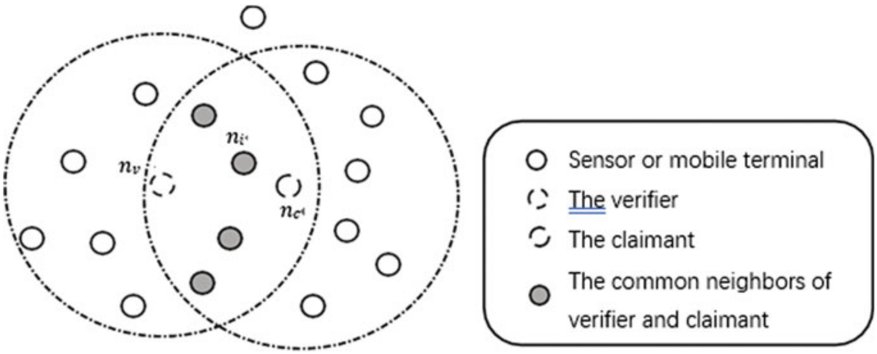
$n_{i'}$
n_v
$n_{c'}$
○ Sensor or mobile terminal
The verifier
The claimant
● The common neighbors of verifier and claimant

Fig. 2. Sensors and mobile terminals in network

We assume the speed of n_v,n_c, and n_i are s_v, s_v and s_i, respectively, which the unit is m/s. The speed difference level γ is calculated by the following equation:

$$\gamma_i = 1 - \frac{|s_v - s_i| + |s_v - s_i|}{2s_i} \tag{2}$$

The distance difference between the verifier and claimant level μ is measured with:

$$\mu_i = \frac{r}{d_{v-i} + d_{v-c}} \tag{3}$$

where d_{v-i} is the distance between the verifier and the i-th neighbor, and d_{v-c} is the distance between the claimant and i-th neighbor; the location information is acquired from the GPS. r is the communication range. Hence, the trust value $\mathrm{TV}_{\mathrm{n_i}}$ of the i-th neighbor is represented by Eq. (4):

$$\mathrm{TV}_{\mathrm{n_i}} = \gamma_i + \mu_i + \beta_i \tag{4}$$

2.2 Layer 2: Mutually Shared Token Scheme

As Fig. 2 shows, when the nodes finished the distance filtering, it could collect $\{\mathrm{RV}_i\}$ into a packet $\mathrm{data}_{\mathrm{mst}}^{n_c}$ from the common neighbors, the mutually shared token follows the bellowing calculation:

$$\mathrm{MST}_{n_c} = \{n_i \in \mathrm{SCN}: \quad \mathrm{TV}_{n_i} > \varphi, \quad \mathrm{data}_{\mathrm{mst}}^{n_c} = \sum \mathrm{RV}_i\} \tag{5}$$

where φ is a threshold of trust value depending on the wireless environment, and SCN is the set of common neighbors. And then $\mathrm{data}_{\mathrm{mst}}^{n_c}$ would be sent to n_v. As the packet received by the verifier n_v, the n_v would do mutually shared token in the same way:

$$\mathrm{MST}_{n_v} = \{n_j \in \mathrm{SCN}^*: \quad \mathrm{TV}_{n_j} > \varphi, \quad \mathrm{data}_{\mathrm{mst}}^{n_c} = \sum \mathrm{RV}_j\} \tag{6}$$

and if the MST_{n_c} matched with MST_{n_v} $(\mathrm{MST}_{n_c} = \mathrm{MST}_{n_v})$, the location information of n_c could be accepted and regarded the n_c as the next-hop node.

3 Performance Analysis

We assume that the malicious nodes n_{m_k} fake its location and broadcast a wrong location to the transmission environment $n_{m_k}^*\left\{L_{m_k}^*\right\}$, $L_{m_k}^* \neq L_{m_k}^{\mathrm{true}}$. With the suitable selection of common neighbors, the verifier and the claimant can receive the same MST. However, if a malicious node pretends its position at a wrong place, such as the situation shows in Fig. 3, even it is an SDM attack, it is hard to collect all necessary packets from signed nodes. Hence, the multi-layer location verification system can defense several attacks discussed above.

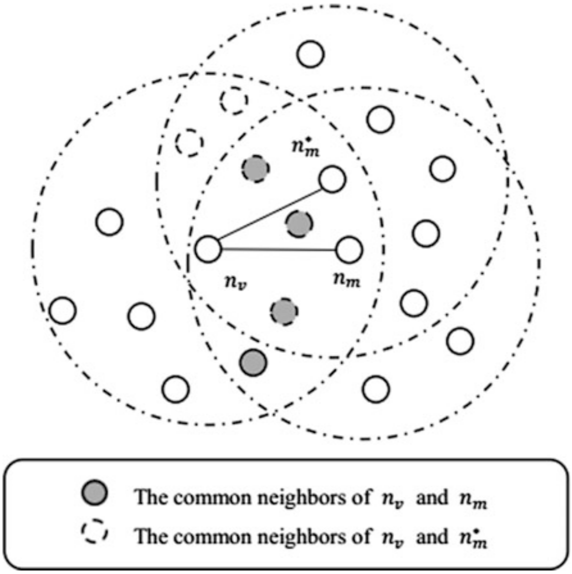
n_m^*
n_v
n_m
● The common neighbors of n_v and n_m
◌ The common neighbors of n_v and n_m^*

Fig. 3. Mutually shared region model with malicious nodes

The performance is evaluated in terms of the ability of the malicious nodes rejection and the location error in different situation. The simulations are built on the MATLAB. The parameter of the simulation is shown in Table 1 which is similar to the [15].

Table 1. Parameters of the simulation

Parameters	Values	Parameters	Values
Simulation area	1000 × 1000 m^2	Propagation	Shadowing
Nodes' speed	0–10 m/s	MAC data rate	10 Mps
Simulation time	20	MAC protocol	IEEE 802.11
Number of nodes	0–500 nodes	Frequency	5.9 GHz
Sources and destinations	20 nodes	Packet type	UDP
Transmission range	150 m	Packet size	512 bytes

The ability of the malicious nodes' defense means that the probability of location error has been discovered under the MLVS. It is assumed that the total number of the malicious nodes is N_m, and the times that packets sent to a malicious node in *i-th* simulation can be regarded as T_m^i. Then the location error e_L happened in the MANETs with multi-layer location verification is following the equation:

$$e_L(\%) = \left\{ \frac{\sum_{i=1}^{20} \frac{T^i_{m\cdot}}{N_m}}{20} \right\} \times 100 \tag{7}$$

In addition, we assume that a single-fake location error in this simulation. Single-fake location error is considered that only one malicious node fakes its location around honest nodes. And Fig. 4a illustrates the performance of MLVS in MANETs with different maximum nodes which contains 10%, 20%, and 30% malicious nodes respectively. The MLVS is a location verification scheme which verifies nodes relying on the neighbors' information; thus, the density of the MANETs deeply impacts the performance of the system. As Fig. 4a shows, the system has a lower location error as the maximum number of nodes is more than 400.

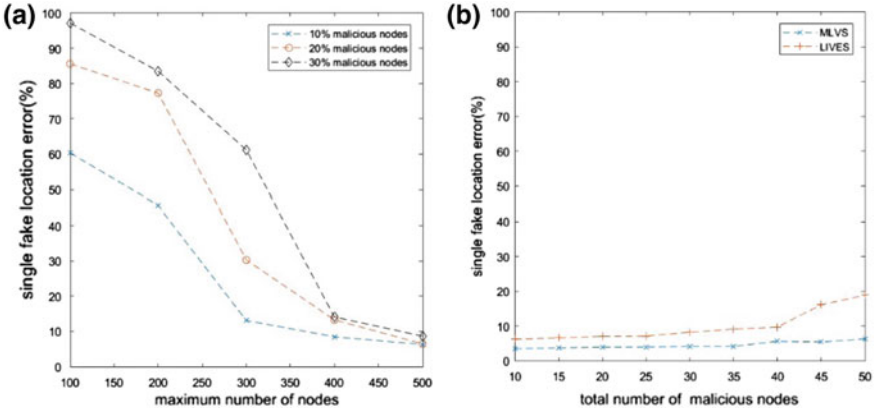

Fig. 4. **a** Performance of MLVS with difference number of malicious nodes and **b** the performance of MLVS compares with LIVES

In Fig. 4b, it shows the performance of MLVS with different number of malicious node and the maximum number of nodes is 500 compared with LIVES illustrated in [15]. In LIVES, the number of malicious nodes impacts the probability of fake position rejection. However, the MLVS has a stable performance with higher node density.

4 Conclusion

In this paper, a multi-layer location verification technique is discussed based on geographic routing in MANETs. The first layer performs a distance filtering for verifiers and claimants and then calculates the trust value for their neighbors as the preparation of common neighbor selection. The second layer evaluates the information collected from common based on the principle of mutually shared token. The trust value calculated in layer one considers the mobility of the network to ensure the verifier, and the claimant can collect information from the same group of neighbors. The MLVS shows a good performance with high-density network; however, it cannot be deployed in sparse MANETs or higher mobility ad hoc networks, such as VANETs. In future, an improved location verification system for VANETs will be considered with the concept of cooperative position.

References

1. Tippenhauer NO, Rasmussen KB, Pöpper C, Capkun S. iPhone and iPod location spoofing: attacks on public WLAN-based positioning systems. SysSec technical Report. Swiss Federal Institute of Technology; 2012 Apr. 2008.
2. Malaney RA. A location enabled wireless security system. In Global telecommunications conference, 2004. GLOBECOM'04. IEEE; 2004. pp. 2196–200.
3. Faria DB, Cheriton DR. Detecting identity-based attacks in wireless networks using signalprints. In Proceedings of the 5th ACM workshop on wireless security; 2006. pp. 43–52.
4. Papadimitratos P, Gligor V, Hubaux JP. Securing vehicular communications-assumptions, requirements and principles. Proc ESCAR. 2006:5–14.
5. Papadimitratos P, Buttyan L, Holczer T, Schoch E, Freudiger J, Raya M, Hubaux JP. Secure vehicular communication systems: design and architecture. IEEE Commun Mag. 2009;46 (11):100–9.
6. Bauer K, McCoy D, Anderson E, Breitenbach M, Grudic G, Grunwald D, Sicker D. The directional attack on wireless localization: how to spoof your location with a tin can. In: Proceedings of the 28th IEEE conference on global telecommunications; 2009. pp. 4125–30.
7. Yan S, Malaney R. Location verification systems in emerging wireless networks. arXiv preprint; 2013 arXiv:1307.3348.
8. Abumansoor O, Boukerche A. A secure cooperative approach for nonline-of-sight location verification in VANET. IEEE Trans Veh Technol. 2012;61(1):275–85.
9. Vora A, Nesterenko M. Secure location verification using radio broadcast. IEEE Trans Dependable Secure Comput. 2006;3(4):2006.
10. Kaiwartya O, Kumar S. Cache agent-based geocasting in VANETs. Int J Inf Commun Technol. 2015;7(6):562–84.
11. Suthaputchakun C, Sun Z. Routing protocol in intervehicle communication systems: a survey. IEEE Commun Mag. 2011;49(12):150–156.
12. Ansari K, Feng Y, Singh J. Study of a geo-multicast framework for efficient message dissemination at unmanned level crossings. IET Intell Transp Syst. 2013;8(4):425–34.
13. Cao Y, Sun Z, Wang N, Riaz M, Cruickshank H, Liu X. Geographic-based spray-and-relay (GSaR): an efficient routing scheme for DTNs. IEEE Trans Veh Technol. 2015;64(4): 1548–64.
14. Kim IH, Kim BS, Song J. An efficient location verification scheme for static wireless sensor networks. Sensors. 2017;17(2):225.
15. Kargl F, Klenk A, Schlott S. Weber M. Advanced detection of selfish or malicious nodes in ad hoc networks. In: European workshop on security in Ad-hoc and sensor networks; 2014. pp. 152–165.