Reliable Mutual Node Evaluation for Trust-Based OLSR in Tactical MANETs

Ji-Hun Lim[1], Keun-Woo Lim[2], and Young-Bae Ko[1](✉)

[1] Ajou University, Suwon, Kyeonggi-do, South Korea
{limbee94,youngko}@ajou.ac.kr
[2] Telecom Paristech, INFRES, RMS, 75013 Paris, France
keunwoo.lim@telecom-paristech.fr

Abstract. This paper proposes a mutual node evaluation method in mobile ad hoc networks to recognize and reliably remove attacker nodes from deteriorating the network. We focus on a tactical networking environment, where the network is generally maintained in harsh and hostile areas while the applications require stringent service requirements. In these kinds of environments, it is desirable to utilize proactive routing methods such as Optimized Link State Routing (OLSR). However, OLSR have weaknesses against various security attacks. To solve this problem, we provide a trust-based evaluation approach where node evaluate each other based on the packet forwarding capabilities. We prove the performance of our proposed method through NS-3.

Keywords: Trust-based routing · Mobile ad hoc networks
Tactical networks · Optimized Link State Routing

1 Introduction

In a tactical Mobile Ad Hoc Networks (MANET), mobile nodes with wireless transmission capabilities, such as soldiers, vehicles, drones, and command centers are required to share and disseminate various tactical information. As the nature of the network tends to have high and frequently changing mobility, how to ensure reliability and connectivity of the network is of utmost priority in this area of research. To provide these capabilities, much research have been progressed in the area of wireless routing protocols, which allows multi-hop communication between tactical nodes on the battlefield.

One of the often considered wireless routing protocol for tactical MANETs is Optimized Link State Routing (OLSR) [1,2]. In the main procedure of OLSR, all nodes participating in the network periodically undergo a HELLO message broadcast and then a multipoint relay (MPR) selection process which structures a multi-hop routing table with the MPRs managing the link-state information. Then, a Topology Control (TC) message exchange is made by all MPRs to share

L. Wang et al. (Eds.): QShine 2017, LNICST 234, pp. 114–119, 2018.
https://doi.org/10.1007/978-3-319-78078-8_12

each of their link information. This allows proactive creation and management of multi-hop routes to all nodes. Therefore, OLSR is considered to be beneficial for time-critical applications, such as tactical MANETs.

However, OLSR is also known to have risks and issues regarding security and trust, and reliability. These include link and identity spoofing attacks [3], wormhole attacks [4], HELLO and TC message tempering [2], and etc. In this paper, we focus on two specific categories of risks.

Denial-of-Service (DoS) Attacks: We specifically focus on nodes that may perform DoS attacks such as a blackhole attack [5] and node isolation attack [6]. Especially in OLSR, in the case of blackhole attack, a malicious node can prioritize itself to become a MPR and drop all packets instead of relaying them. In the case of a node isolation attack, the malicious node can advertise its TC message without the information of nodes that use itself as MPR which means that these nodes will become invisible to the entire network.

Mobility and Reliability Issues: Even if nodes are not attackers, specific nodes may not be reliable due to being located at or moving to unfavorable locations. It is important to be able to isolate these nodes from becoming MPRs. Li et al. [7] states that mobility affects the performance of MPR forwarding, and proposes a method of modeling the mobility of nodes and calculating the chances of a node becoming a MPR through this mobility model.

In this paper, we focus on mutual node evaluation to create a trust-based OLSR for tactical MANETs. To prevent the two risks mentioned above, we propose a trust-value based approach where each node evaluates all other nodes in the network using a trust-value. Based on these trust values during MPR selection, only nodes that are deemed trustworthy will be selected as MPRs. Successful data forwarding will award nodes into having a higher trust, while continuous failure in data transmission will degrade the trust of the node, eventually isolating the node from MPR selection.

2 Mutual Node Evaluation Method

The general procedure of our proposed mutual node evaluation method is progressed by adding and maintaining a *trusttable* to each node in the network. By sharing and referencing other nodes' trust values of all the other nodes, evaluation becomes mutual; henceforth the name of our method. There are four sequences of operations in the proposed scheme: (1) Creation and management of trust table, (2) Selection of MPR, (3) Recalculating the trust value, and (4) Extension of TC message for sharing trust value.

2.1 Creation and Management of Trust Table

In the initial phase of the OLSR, each node creates what we define as a *trust table*. The size of a trust table is defined as $m * m$, where m is the number of all nodes in the network. Each entry in the trust table is the *trust value*, which defines how much a node (in the row) trusts another node (in the column). From here onwards, we denote the trust value of node a to node b as $T_{a \to b}$. In the initial stage, the node will record a trust value of 100 to all other nodes, while keeping the evaluation of other nodes to $NULL$.

This table is updated whenever TC message is shared between all the nodes, where the trust table of each node is included in the TC message and exchanged. For example, if node b broadcasts its TC message, it includes $T_{b \to a}$, $T_{b \to b} = NULL$, $T_{b \to c}$, $T_{b \to d}$, and $T_{b \to e}$ values in the message. Once node a receives this message, it can update the trust table. The result of node a first generating its table and updating it can be observed in Table 1. A node will not send its trust value of itself as this value will not be used. Note that the values are all recorded in Table 1 are 100 or $NULL$ because it is an example of initial phase.

Table 1. Trust table of node a after receiving TC message from node b

	a	b	c	d	e
a	100	100	100	100	100
b	100	$NULL$	100	100	100
c	$NULL$	$NULL$	$NULL$	$NULL$	$NULL$
d	$NULL$	$NULL$	$NULL$	$NULL$	$NULL$
e	$NULL$	$NULL$	$NULL$	$NULL$	$NULL$

2.2 Trust-Based MPR Selection

Using the trust table, each node needs to select MPR nodes to forward its data. To do this, each node calculates the *aggregated* trust value of all 1-hop neighbors and chooses only the nodes with high aggregated trust values as MPRs. For example, if node a needs to calculate aggregated trust value $R_{a \to b}$ of a neighbor node b, Eq. 1 is used:

$$R_{a \to b} = (\sum_{x=1}^{n'} T_{x \to b})/n' \tag{1}$$

where n is the number of 1-hop neighbors and n' is the number of 1-hop neighbors with non $NULL$ value during the calculation of $R_{a \to b}$. After calculating aggregated trust values for all n, the node can select either the node with the highest value as MPR or even select multiple MPRs with satisfactory trust values if multiple MPRs are needed to maintain connectivity.

We elaborate on the calculation of aggregated trust values here with an example. Let us assume that node a maintains a trust table as shown in Table 2.

When node a calculates the aggregated trust values, $R_{a \to b} = (100 + 80)/2 = 90$, $R_{a \to c} = 100 + 100/2 = 100$, $R_{a \to d} = 100 + 90 + 90/3 = 93.3$, and $R_{a \to e} = 100 + 90 + 75/3 = 83.3$. Therefore, for node a, node c will become its MPR. Note that all nodes, using its own trust table, will each make this calculation periodically to choose the MPR.

Table 2. Example of a trust table state of node a

	a	b	c	d	e
a	100	100	100	100	100
b	100	$NULL$	100	90	90
c	90	80	$NULL$	90	75
d	$NULL$	$NULL$	$NULL$	$NULL$	$NULL$
e	$NULL$	$NULL$	$NULL$	$NULL$	$NULL$

2.3 Recalculating the Trust Value

Once the MPR is selected for all nodes, the network will function with this configuration until the next period of new MPR selection. Before selecting a new MPR, each node will evaluate the performance of its MPR. To do this, we apply a cross-layer approach of deciding whether a data packet has been successfully transmitted on a end-to-end basis.

For transport protocol, if the transmission control protocol (TCP) [8] is used, the acknowledgment (ACK) can be used to check if a data transmission of a node has been successfully transmitted multi-hop to its destination. Using the ACK message, it is possible to calculate the current data rate of transmission and compare with the data rate requirements of the service application. If the data rate meets the requirements, then the MPR can be considered reliable and given an incentive to its trust value. On the other hand, if the requirements are not met, then the trust value will be given a penalty. If a protocol without ACK is used at the transport layer, it is possible to provide a simple ACK function on the application layer to calculate the data rate of a node's transmission.

Note that for our current implementation of the protocol, we have made some preliminary empirical analysis of the appropriate incentive and penalty values, and configure the settings to 5% and 10%. As an example, if node b was given a 5% incentive by node a, $T_{a \rightarrow b} = 95 * 1.05 = 99.75$. Through TC message sharing, this information will be shared to other nodes in the network. Therefore, malicious nodes, whether they are DoS attackers or under-performing nodes, can be naturally deteriorated and isolated from the network.

2.4 Extension of TC Message

The trust values of a node will be shared through periodical TC message exchange, which is already a default procedure in OLSR. However, to include this information, TC message needs to be extended. This can be simply done as TC messages are bound to change in size frequently due to the size of the topology that each node has to advertise. Therefore, it is convenient to add the information of a node's trust table (Only the information of its own trust values) on the end of the TC message. In our implementation we add the IPv4 address of each node, followed by the trust value in 4 bytes. Therefore, the induction of additional overhead in the TC message will be $(4bytes + 4bytes) * m$. We consider this much more acceptable than having to create another packet format exclusively to share trust table values.

3 Performance Evaluation

The performance of our mutual node evaluation method in OLSR is evaluated through NS-3 simulation. For our preliminary evaluation, we set our tactical environment as shown in Table 3.

Table 3. Simulation environment

Parameter	Value
PHY/MAC	IEEE 802.11a 54 Mbps
Routing	OLSR
Number of nodes	16
Data characteristics	64, 128, 192, 384 Kbps H.264 encoding
Mobility model	Random walk

The main performance parameter that we consider is number of dropped packets due to attack. As the main effect of black hole attacks and isolation attack both deteriorate the node data transmission, improving this factor was our foremost priority. We compare our method with the original OLSR, which is the most baseline performance. 16 nodes are deployed in a grid topology on a 200 * 200 m space and each node moves randomly along a random walk mobility model. All nodes except the server node and the attacking node transmit multimedia data to the server node. The emulated data format is h.264 Mpeg-4 AVC video, with speeds differing based on screen resolution and frames per second. To receive acknowledgment of the data rate, we also implement a simple ACK mechanism on the application layer. The performance results are shown in

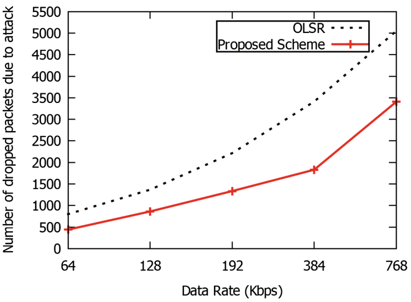

Fig. 1. Number of dropped packets comparison

Fig. 1. Our proposed scheme generally shows lower number of dropped packets than existing OLSR. This is mainly due to our method being able to successfully find and isolate an attacker node. Even though this may result in creation of longer routes because attacker nodes must be avoided, it is more reliable compared to the original OLSR which cannot avoid attacker nodes.

4 Conclusion

In tactical MANETs, security and reliable data delivery are the most important features that need to be guaranteed. To provide this, we propose a mutual node evaluation method based on OLSR protocol to exploit this problem. The performance evaluation shows that our method of detecting malicious nodes is effective in preventing them becoming MPRs in the OLSR algorithm. Note that the simulation results that we have presented are preliminary and we will continue to make more extensive simulation, as well as utilize testbeds to make a more practical environment. Finally, we will analyze methods to tune incentive and penalty values for a more intelligent calculation of the trust values.

Acknowledgement. This research was supported in part by the MIST (Ministry of Science and ICT), Korea, under the National Program for Excellence in SW supervised by the IITP (Institute for Information & communications Technology Promotion) (20150009080031001), and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2015R1D1A1A01059049).

References

1. Clausen, T., Jacquet, P., Laoiti, A., Minet, P., Muhlethaler, P., Qayyum, A., Viennot, L.: Optimized Link State Routing Protocol. IETF Internet Request For Comments RFC 3626 (2003)
2. Ronggong, S., Mason Peter, C.: ROLSR: a robust optimized link state routing protocol for military ad-hoc networks. In: IEEE MILCOM 2010 (2010)
3. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., Jamalipour, A.: SA-OLSR: security aware optimized link state routing for mobile ad hoc networks. In: IEEE ICC 2008 (2008)
4. Hu, Y.-C., Perrig, A., Johnson, D.: Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 370–380 (2006)
5. Gerhards-Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., Tolle, J.: Detecting black hole attacks in tactical MANETs using topology graphs. In: IEEE LCN 2007 (2007)
6. Schweitzer, N., Stulman, A., Shabtai, A., Margalit, R.D.: Mitigating denial of service attacks in OLSR protocol using fictitious nodes. IEEE Trans. Mobile Comput. **1**, 163–172 (2016)
7. Li, Z., Wu, Y.: Smooth mobility and link reliability based optimized link state routing scheme for MANETs. IEEE Commun. Lett. **21**(7), 1529–1532 (2017)
8. Postel, J.: Transmission Control Protocol. Internet Request For Comments RFC 793 (1981)