A Trust Model Focusing on Node Usage in Mobile Ad hoc Networks

Nanaka Asai, Sonoko Goka, Hiroshi Shigeno
Graduate School of Science and Technology
Keio University
3-14-1 Hiyoshi Kohoku-ku
Yokohama-shi Kanagawa Japan
{asai, goka, shigeno}@mos.ics.keio.ac.jp

***Abstract*—Mobile ad hoc networks (MANETs), where nodes can communicate without an infrastructure, require all nodes to be cooperative enough to transfer packets for other nodes. MANETs have been studied for decades, due to its characteristics which are infrastructureless and distributed. However, the existence of malicious nodes that drop packets for their resource protection is one of the important issues of the present research. Reputation systems using trust model have been proposed to detect malicious nodes in MANETs. Here, the trust value indicates the degree of reliance. One of the attacks in MANETs is On-Off attack on which attack nodes keep trust above a certain level by repeating forwarding and dropping packets. In this paper, we propose a trust model focusing on node usage against MANETs On-Off attack (TMUMO). In this study, we detect On-Off attack nodes by considering the characteristics of On-Off attack. Through simulation experiments, we improve detection rate of attack nodes and packet delivery rate in MANETs, and show feasibility of our trust model.**

***Index Terms*—MANETs, trust, secure routing, reputation**

I. Introduction

In recent decades, Mobile ad hoc networks (MANETs) [1] have gained considerable interest and adoption because of their flexibility in various scenes. In MANETs, nodes communicate directly with each other and build a network dynamically. Therefore, MANETs are expected as effective means of communication when infrastructure cannot be used, such as in case of large-scale disaster. However, malicious nodes may improperly drop packets in order to save their resources in MANETs. Various secure routing protocols have been proposed to detect and avoid malicious nodes, such as AOTDV [2], [3], TA-AODV [4]. These secure routing protocols use reputation system which evaluates 1-hop neighbors using trust, and avoid paths in which malicious nodes exist. A node calculates a trust value for each 1-hop neighbor node based on packet relay rate. Trust value becomes higher when a node cooperates with forwarding. If trust value of a node's 1-hop neighbor is lower than a threshold, the node stores the 1-hop neighbor node in the blacklist, and excludes it from the network. In this way, secure routing protocols reduce the impact of malicious nodes, and improve the packet delivery rate in MANETs.

JSPS KAKENHI Grant Number 17KT0082

There are nodes who behave not to be detected as malicious nodes [5]. For example, a Bad Mouthing Attack node improves its trust value by telling trust values of other nodes around lower than actual, and a Conflicting Behavior Attack node keeps its trust value by moving and changing a place where they drop packets and forward packets. On-Off Attack is one of attacks that attack nodes behave not to detect as malicious nodes. On-Off Attack nodes repeat dropping and forwarding packets to keep their trust above a certain level. Moreover, it is difficult to detect an On-Off Attack node because the trust value is hard to fall down, when it gets a lot of packet relay requests. Thus, reputation systems have to be changed depending on the number of packet relay requests.

In this paper, we propose a trust model focusing on node usage against MANETs On-Off Attack (TMUMO). The goal is to detect On-Off Attack nodes, and reduce the impact of malicious nodes by excluding them from the MANETs. This proposal method controls a blacklist threshold dynamically dependent on a node usage which is calculated by the number of packet relay requests. In case of high number of packet relay requests, we detect an On-Off Attack node by raising a blacklist threshold. Moreover, this proposoal method also detect nodes which get a lot of packet relay requests so that they can keep trust above a certain level in spite of dropping some packets.

The remainder of the paper is organized as follows. In section 2, we present the related work. In section 3, the description of our proposed framework is given and in section 4, we explain our simulation environment. A series of simulations are demonstrated in section 5, and finally we conclude and discuss the future work of the paper in section 6.

II. Related Work

In this section, we explain a trust model using with general secure routing in MANETs.

A. Secure Routing Protocol

When a source node sends a packet to a destination node on a path that includes a malicious node, the packet may be dropped by the malicious node and can't reach the destination node. The goal of secure routing protocol is to select a

978-1-5386-9151-9/19/$31.00 ©2019 IEEE

trustworthy path in a realistic environment where malicious nodes exist [6], [7].

Routing protocol using reputation system is one of the secure routing protocols. Reputation system enables source nodes to select secure and reliable paths by using trust which shows node's reliability and detecting malicious nodes [8], [9].

B. Trust Model

A trust value for a node is a value of reliability which is calculated based on their behaviors by 1-hop neighbors of the node. By selecting a node with high trust value as a path, each node can select a secure path and communicate with a destination node.

A node overhears and checks that a 1-hop neighbor of the node relays a packet correctly, and calculates and updates the 1-hop neighbor's trust immediately after it sends a data packet. "Relay a packet correctly" means relay the packet without manipulation or dropping. The trust value depends on the packet forwarding rate, and is defined as the ratio of the number of packets correctly relayed to the total number of packets that received the packet relay request [10]. The trust value is represented from 0 to 1. A node which is cooperative to forward packets has high trust value, on the other hand, a node which is uncooperative to forward packets has low trust value.

C. Blacklist

Blacklist threshold is a threshold used for detecting malicious nodes when the trust values update. Each node detects a 1-hop neighbor node as a malicious node when the 1-hop neighbor node has lower trust value than the blacklist threshold. Each node doesn't forward a packet which is sent by a node in its blacklist. Moreover, it doesn't send a packet to a node in its blacklist except broadcast packets. Thus, when a node is stored in all nodes' blacklists, it is completely excluded from the network.

By using a blacklist, it is possible to exclude malicious nodes from the network, and to communicate with each node by using secure and reliable paths.

III. Problems in Existing Secure Routing Protocol

In MANETs, there are various attacks. In this paper, the number of communications means number of times selected for the relay node. The existing secure routing protocols don't consider On-Off Attack nodes which repeat forwarding and dropping packets and keep trust above a certain level [11]. When the number of communications is high, even if intentional packet dropping is performed, it is difficult to detect as a malicious node because the trust value is hard to fall down. In this paper, we discuss these two problems as On-Off Attack problem and detection problem, and examine causes and impact of these on the network.

A. On-Off Attack Problem

On-Off Attack [5] is an attack that an attack node keep its trust above a certain level by repeating packet forwarding and dropping at regular time intervals. Hence the existing secure routing protocols use constant blacklist thresholds, they can't detect On-Off Attack nodes. When they misdetect On-Off Attack nodes as cooperative nodes, it may happens that attack nodes drop packets. Moreover, it is assumed that cooperative nodes forward packets from On-Off Attack nodes to other nodes, and forward packets to On-Off Attack nodes. Thus, in MANETs in which nodes have limitations of their resources, cooperative nodes run extra resources, and performance of the whole network deteriorates. Therefore, On-Off Attack Problem is an issue to be solved.

B. Detection Problem

The trust value is the value of reliability of a node which is calculated on the basis the node's behaviors observed by a 1-hop neighbor, and shows a ratio of the number of packets correctly relayed to the total number of packets requested to be relayed. When the number of communications is low, the trust value fluctuates significantly. Thus, when the number of communications is low and packet loss due to communication error happens, the trust value decreases greatly and the node may be detected as a malicious node. While, when the number of communications is high and a node drops packets intendedly, the trust value decreases slightly and it is difficult to detect the node as a malicious node. At trust model of the existing secure routing protocol, a blacklist threshold is a constant, not dependent on the number of communications. In case of a blacklist threshold is low, the former problem is solved, but malicious node detection rate will be decreased in the whole network. On the other hand, in case of a blacklist threshold is high, the latter problem is solved and malicious node detection rate is improved, but it assumed that a cooperative node is misdetected as a malicious node due to unintended packet losses. From the above, we assume the performance of the entire network is degraded by using a blacklist threshold not dependent on the number of communications. Therefore, detection problem is an issue to be solved.

IV. TMUMO

We propose a trust model focusing on node usage against MANETs On-Off attack to manage On-Off attack problem and detection problem. In this section, we explain our scheme TMUMO.

A. Overview of Our Proposal

TMUMO introduces node usage to solve On-Off attack problem and detection problem. A node usage U_{ij} is a value which represents degree of node j selected by node i as a packet relay node and is represented from 0 to 1. High U_{ij} value shows that node i selected node j as a packet relay node many times.

Node j is a 1-hop neighbor node of node i. First, node i requests node j to relay a packet. Second, node i overhears to checks if node j correctly relayed the packet, and calculates the trust value for node j, i.e., T_{ij}. Third, node i calculates the node usage U_{ij} from the past number of communications

with node j, and decides the blacklist threshold B_{ij}. Finally, compared with the blacklist threshold B_{ij} and the trust value T_{ij}, if the trust value is lower than the blacklist threshold, node i detects node j as a malicious node and stores node j in its blacklist.

B. Proposal Details

1) Calculation of the Trust Value T_{ij}: Node i calculates the trust value T_{ij} for node j from the node j's packet relay rate. Node i overhears to check if node j relays the packet correctly, and calculates and updates the trust value T_{ij}. The trust value T_{ij} shows the packet forwarding rate, and is as the ratio of node j's number of packets correctly relayed to the total number of packets requested to be relayed from node i. The node j's trust value T_{ij} calculated by node i is given by the following equation:

$$T_{ij} = \frac{\alpha_{ij} + \eta}{(\alpha_{ij} + \eta) + (\beta_{ij} + \sigma)}, \tag{1}$$

where α_{ij} is the number of times that node j relays node i's packets correctly, β_{ij} is the number that node j drops node i's packets, η is the initial value of relaying packets correctly, and σ is the initial value of dropping packets ($\eta \geq 1 \cap \sigma \geq 1$). By defining the initial values, we can calculate the trust value of not communicated node. The trust value T_{ij} is the value between 0 to 1. Accordingly, T_{ij} is high when node j is cooperative in forwarding packets.

2) Calculation of the Node Usage U_{ij}: The node usage U_{ij} is a value which represents degree of node j selected by node i as a packet relay node and is represented from 0 to 1. The node usage U_{ij} is high when node i selects node j as a packet relay node many times. The node j's usage U_{ij} calculated by node i is given by the following equation:

$$U_{ij} = 1 - \frac{\gamma}{\alpha_{ij} + \beta_{ij} + \gamma}, \tag{2}$$

where α_{ij} is the number that node j relays node i's packets correctly, β_{ij} is the number that node j drops node i's packets, and γ is a constant ($\gamma > 0$) . The node usage U_{ij} is the value more than 0 and less than 1. Accordingly, the node usage U_{ij} is high, when node i selects node j as a packet relay node many times. Moreover, the node usage U_{ij} grows slowly when γ in equation(2) is low. On the other hand, the node usage U_{ij} grows quickly when γ in equation(2) is high.

3) Calculation of the Blacklist Threshold B_{ij}: The blacklist threshold B_{ij} is the threshold that node i detects node j as a malicious node. When the trust value T_{ij} is lower than the blacklist threshold B_{ij}, node i detects node j as a malicious node. The blacklist threshold B_{ij} is calculated by using the node usage U_{ij}.

The node j's blacklist threshold calculated by node i is given by the following equation:

$$B_{ij} = U_{ij} \times \rho, \tag{3}$$

Where ρ is a constant ($0 < \rho \leq 1$) . Accordingly, the blacklist threshold B_{ij} is proportional to the node usage U_{ij}.

when the node usage U_{ij} is low, the blacklist threshold B_{ij} is low and node i doesn't detect as a node j even if node j's trust value is low. On the other hand, when the node usage U_{ij} is high, the blacklist threshold B_{ij} is low and node i check node j severely. Besides, when the value of ρ is high, the blacklist threshold changes significantly dependent on the node usage, and when the value of ρ is low, the blacklist threshold changes slightly depend on the node usage. Moreover, the blacklist threshold B_{ij} is $0 \leq B_{ij} < \rho$, because the node usage U_{ij} is 0 or more and less than 1.

C. Application to Secure Routing Protocol

The trust model TMUMO can be applied to various secure routing protocols. We explain how to apply TMUMO to existing routing protocol AODV.

Step 1: A source node i sends a packet to node j. Node i overhears node j's packet relay and updates its trust record table.
Step 2: Following the updated trust record table, node i calculates node j's trust T_{ij} by using equation(1).
Step 3: Node i calculates node j's node usage U_{ij} by using equation(2).
Step 4: Node i calculates node j's blacklist threshold B_{ij} by using equation(3).
Step 5: Node i compares the trust value T_{ij} with the blacklist threshold B_{ij}. If the trust value T_{ij} is higher than B_{ij}, node i judges node j as a cooperative node and finishes this process. Otherwise, node i stores node j in its blacklist and finishes this process.

V. Simulation Environment

We present the trust model focusing on node usage against MANETs On-Off attack (TMUMO). In order to show the usefulness of the proposed method TMUMO, evaluation was performed by simulation reproducing the environment where On-Off attack or random packet drop attack occurs.

A. Simulation Model

We used network simulator Qualnet [12] for evaluation. In evaluating the proposed method, we confirmed the difference in the proposed method TMUMO compared with the secure routing AOTDV [2] using the existing trust model. Table I shows simulation parameters, and table II and table III show specific simulation parameters in AOTDV or TMUMO. Parameters in table I and II are along the parameters in AOTDV [2] and the parameters in table III was decided by carrying out preliminary simulations.

B. Node Behavior Models

Following two are node behavior models.

1) Cooperative Node: An cooperative node forwards all packets correctly. This node behaves cooperatively with the network without packet dropping and manipulation.

TABLE I
COMMON SIMULATION CONDITIONS

Simulator	Qualnet 6.1
Simulation time	3600 sec
Number of nodes	50
Wireless standard	IEEE 802.11n
Map size	1000m × 1000m
Transfer range	250m
Transmission power	20dBm
Traffic type	CBR (UDP)
Packet size	512 byte
Packet rate	1 pkts/s
Mobility model	Random waypoint

TABLE II
SIMULATION CONDITIONS ON AOTDV

Initial value of trust T_{ini}	0.75
Blacklist threshold B_{ij}	0.4
Initial value of packet transfer count	3
Initial value of packet relay request count	4

2) Malicious Node: A malicious node drops packets received from others depending on packet dropping rate, while it forwards its own packet such that it is a source node or a destination node. However it forwards control packet correctly.

On-Off Attack

An attack node tries to keep its trust value above a certain level by repeating packet forwarding and dropping at regular time intervals.

Random Packet Drop Attack

An attack node tries to keep its trust value above a certain level by dropping packets randomly depending on packet dropping rate.

C. Evaluation Metrics

We use the following metrics to evaluate the performance of the protocols.

1) Average detection rate of malicious nodes (AD): The average fraction of malicious nodes detected by each normal node to the total number of malicious nodes.

2) Packet delivery rate(PDR): The fraction of the data packets delivered by normal source nodes to destination nodes to all data packets sent by normal source nodes.

VI. SIMULATION RESULT AND ANALYSYS

Impact of packet dropping rate of attack nodes:

We compare TMUMO and AOTDV in the condition of varying malicious nodes' packet dropping rate. The maximum speed of the nodes is from 0m/s to 5m/s, the number of attack nodes is 20, and the On-Off attack cycle is 10 seconds. We change the packet dropping rate of the attack nodes from 0% to 100%.

A. Average Detection rate of Malicious Nodes (AD)

On-Off Attack: Figure 1 shows the average detection rate of malicious nodes depending on change of On-Off attack nodes' packet dropping rate. In figure 1, AOTDV increases the detection rate depending on increasing of attack nodes' packet dropping rate. When the packet dropping rate is high, the trust value becomes low. Therefore AOTDV can detect malicious nodes, when the trust values of the nodes becomes 0.4 or less.

TABLE III
SIMULATION CONDITIONS ON TMUMO

Initial value of trust T_{ini}	0.5
η in equation(1)	1
σ in equation(1)	1
γ in equation(2)	10
ρ in equation(3)	0.9

On the other hand, TMUMO always has higher detection rate of malicious nodes than AOTDV. Especially, average detection rate of TMUMO is $19pt$ higher than that of AOTDV when the packet dropping rate of malicious nodes is 40%. The reason for the increasing of the average detection rate when the packet dropping rate is from 20% to 40% is that the AOTDV's blacklist threshold is 0.4. Therefore AOTDV has difficulty to detect nodes with packet dropping rate between 0% and 60% as malicious nodes. On the other hand, TMUMO can detect On-Off attack nodes which keep the trust values above a certain level because TMUMO increase a blacklist threshold with a node usage.

As a result, TMUMO improves average detection rate of On-Off attack nodes by up to $19pt$ compared with AOTDV.

Random Packet Drop Attack: Figure 2 shows the average detection rate of malicious nodes depending on change of the packet dropping rate of random packet drop attack nodes. In figure 2, AOTDV increases the detection rate depending on increasing of the packet dropping rate of the attack nodes. When the packet dropping rate is high, the trust value becomes low. Therefore AOTDV can detect malicious nodes, when the trust values of the nodes becomes 0.4 or less. On the other hand, TMUMO always has higher detection rate of malicious nodes than AOTDV. Especially, the average detection rate of TMUMO is $30pt$ higher than that of AOTDV when the packet dropping rate of malicious nodes is 40%. AOTDV can't detect 20% random packet drop attack nodes as malicious nodes because AOTDV use a constant as the blacklist threshold. On the other hand, TMUMO can detect 14% of malicious nodes with 20% packet dropping rate because TMUMO increases the blacklist threshold with increasing the node usage and checks severely if the node is malicious.

As a result, TMUMO improves the average detection rate of random packet drop attack nodes by up to $30pt$ compared with AOTDV.

B. Paket Delivery Rate (PDR)

On-Off Attack: Figure 3 shows the packet delivery rate depending on change of On-Off attack nodes' packet dropping rate. Both TMUMO and AOTDV drop the packet delivery rate as the packet dropping rate of malicious nodes rises. TMUMO has the same or high packet delivery rate compared

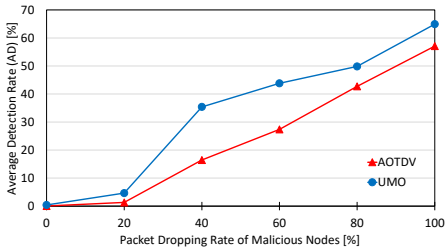

Fig. 1. Average detection rate in On-Off attack

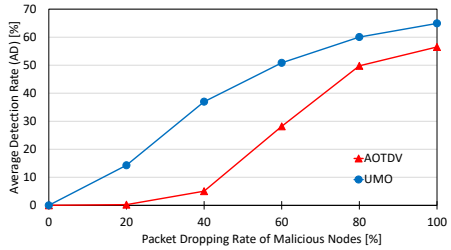

Fig. 2. Average detection rate in random packet drop attack

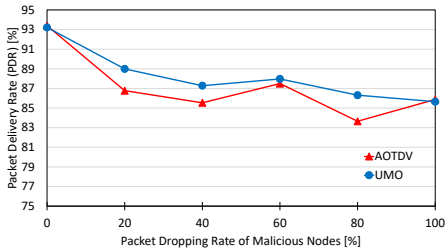

Fig. 3. Packet delivery rate in On-Off attack

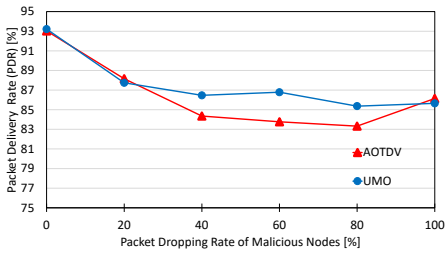

Fig. 4. Packet delivery rate in random packet drop attack

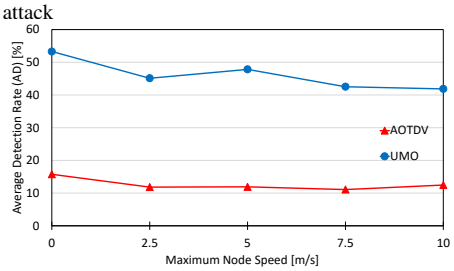

Fig. 5. Average detection rate in random packe drop attack

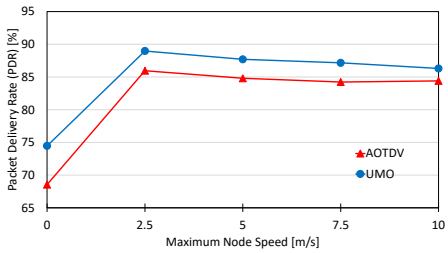

Fig. 6. Packet delivery rate in random packet drop attack

with AOTDV. When the packet dropping rate of malicious nodes rises, the packet delivery rate drops because malicious nodes drop many packets.

AOTDV has difficulty to detect malicious nodes with the packet dropping rate of 60% or less because the blacklist threshold of AOTDV is 0.4. Therefore AOTDV can't exclude malicious nodes from the network and the packet delivery rate of AOTDV is dropped. In addition, AOTDV improves the detection rate but the packet delivery rate drops as a whole network because undetected malicious nodes' packet dropping rate rises when the packet dropping rate is more than 60%.

On the other hand, TMUMO can detect On-Off attack nodes with high node usages because TMUMO increases the blacklist thresholds to the nodes with high node usages. Therefore TMUMO excludes malicious nodes from the network, and has high packet delivery rate compared with AOTDV. Especially, TMUMO improves packet delivery rate by up to $3pt$ compared with AOTDV when the packet dropping rate of malicious nodes is 80%.

Random Packet Drop Attack: Figure 4 shows the packet delivery rate depending on change of random packet drop attack nodes' packet dropping rate. Both TMUMO and AOTDV drop packet delivery rate as packet dropping rate of malicious nodes rises. TMUMO has same or high packet delivery rate compared with AOTDV. When the packet dropping rate of malicious nodes rises, the packet delivery rate drops because malicious nodes drop many packets.

AOTDV has difficulty to detect malicious nodes with packet dropping rate of 60% or less because the blacklist threshold of AOTDV is 0.4. Therefore AOTDV can't exclude malicious nodes from the network and the packet delivery rate of AOTDV is dropped. In addition, AOTDV improves the detection rate but the packet delivery rate is dropped as a whole network because undetected the packet dropping rate of malicious nodes rises when the packet dropping rate is more than 60%.

On the other hand, TMUMO can detect random packet drop attack nodes with high node usages because TMUMO increases the blacklist threshold to the nodes with high node usage. Therefore TMUMO excludes malicious nodes from the network, and has high packet delivery rate compared with AOTDV. Especially, TMUMO improves the packet delivery rate by up to $5pt$ compared with AOTDV when the packet dropping rate of malicious nodes is 80%.

Impact of nodes' mobility:

We compare TMUMO and AOTDV in the condition of varying maximum speed of nodes. The number of attack nodes is 20, the packet dropping rate of the attack node is 50%, and the attack model is random packet drop attack.

C. Average Detection rate of Malicious Nodes (AD)

Figure 5 shows the average detection rate of malicious nodes depending on change of nodes' maximum speed. In figure 5, AOTDV is nearly constant at 13% not depending on nodes' maximum speed. Therefore there is no dependence on nodes' maximum speed and the average detection rate of malicious nodes in AOTDV. As the maximum speed of the nodes increases, there is a possibility that the detection rate decreases because there is a node that moves outside the communication range before detecting it as an attack node in this simulation. Since the node moves within the map of 1000m × 1000m, the possibility of the node moving outside the communication range is low. On the other hand, TMUMO always has the higher detection rate of malicious nodes than that of AOTDV, and drops it with increasing nodes' maximum speed. Comparing the maximum speed by 0m/s and the maximum speed by 10m/s, the detection rate

of malicious nodes decreases by about $10pt$. TMUMO uses node usages for calculating blacklist thresholds. In the absence of node mobility, a topology of a node does not change, so the node always requests packet relay to the same 1-hop node. Therefore, the node usage rate rises immediately and the black list threshold also rises, making it easier to detect attack nodes. Moreover, TMUMO has improved the average detection rate by about $40pt$ compared with AOTDV. This is because TMUMO raises the black list threshold for nodes with high node usage and severely detects attack nodes.

From the above results, we confirmed that TMUMO improved the average detection rate of malicious nodes by up to $40pt$ compared with AOTDV.

D. Paket Delivery Rate (PDR)

Figure 6 shows the packet delivery rate depending on change of the maximum speed of nodes. In AOTDV, the packet delivery rate is the lowest when the maximum speed of the nodes is 0m/s, and is the highest when the maximum speed of nodes is 2.5m/s. When the maximum speed of nodes is 0m/s, the number of hops from the source node to the destination node is large. Therefore the packets are discarded due to problems such as TTL. The reason why the packet delivery rate tends to decrease between by 2.5m/s and by 10m/s is that the route is not well designed due to node mobility problems and the packet is discarded. On the other hand, TMUMO has improved the packet delivery rate of about $6pt$ at maximum compared to AOTDV. TMUMO can increase the packet delivery rate because TMUMO can select a safer route by raising a blacklist threshold according to a node usage, detecting an attack nodes and excluding it from the network.

Based on the above results, TMUMO has confirmed that it improves the packet arrival rate by detecting attack node compared with AOTDV.

VII. Conclusion

In this paper, we proposed the trust model focusing on node usage against MANETs On-Off attack (TMUMO). TMUMO introduces the node usage which is calculated by a 1-hop neighbor node from the number of received packet relay requsts. TMUMO increases a node usage with the number of times selected as a packet relay node. In addition, TMUMO controls a blacklist threshold dynamically depending on the node usage. A blacklist threshold is low when a node has a low node usage, and a blacklist threshold is high when a node has a high node usage. Therefore TMUMO can detect malicious nodes effectively which have the high number of communications and drop packets improperly. Moreover TMUMO can detect On-Off attack nodes which keep the trust values above a certain level by repeating packet dropping and forwarding at regular time intervals.

In order to show the efficiency of the proposed method TMUMO, evaluation was performed by simulation reproducing the environment where On-Off attack or random packet drop attack occurs. Compared with AOTDV, TMUMO has improved the average detection rate of On-Off attack nodes by up to $19pt$ and improved that of random packet drop attack by up to $30pt$. Thus TMUMO has improved the packet delivery rate by up to $3pt$ in case of On-Off attack and by up to $5pt$ in the case of random packet drop attack. Moreover TMUMO has reduced the effect of mobility compared with AOTDV. When the maximum speed of nodes has changed, TMUMO has improved average detection rate by up to $40pt$ and improved packet delivery rate by up to $6pt$ compared with AOTDV. As a result, TMUMO can reduce the impacts of On-Off attack problem and Detection problem by detecting malicious nodes effectively compared with AOTDV.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number 17KT0082. We acknowledge the stimulated discussion in the meeting of the Cooperative Research Project of the Research Institute of Electrical Communication, Tohoku University.

References

[1] S. Corson and J. Macker, *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*, RFC 2501 (Informational), (1999).

[2] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, Trust-based on-demand multipath routing in mobile ad hoc networks, 技術評論社 nformation Security, IET, Vol. 4, No. 4, pp.212-232(2010).

[3] H. R. Karande and S. A. Thorat, Performance analysis of ftdsr and aotdv trust based routing protocols, Eleventh International Conference on Wireless and Optical Communications Networks(2014).

[4] H. Ushikubo, S. Takeda, and H. Shigeno, "An effective secure routing protocol considering trust in mobile ad hoc networks," vol. 55, no. 2, pp. 649658, 2014 (in Japanese).

[5] A.A. Pirzada, C. McDonald, and A. Datta, Trust-distortion resistant trust man-agement frameworks on mobile ad hoc networks: A survey, IEEE Communications Surveys and Tutorials,(2016).

[6] S.A. Thorat and P.J. Kulkarni, Design issues in trust based routing for manet, In Computing, Communication and Networking Technologies(2014).

[7] Yuri Ohata, Takashi Kamimoto, Ryoki Shinohara, and Hiroshi Shigeno, Cooperation incentive system balancing virtual credit in mobile ad hoc networks, In Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 218-226,(2016).

[8] Huaizhi Li and M. Singhal, Trust management in distributed systems, Computer, Vol. 40, No. 2, pp. 45-53(2007).

[9] P. Mitra and S. Mukherjee, A review of trust based secure routing protocols in manets, In 2015 International Conference and Workshop on Computing and Com- munication, pp.1-7(2015).

[10] Chi Zhang, Xiaoyan Zhu, Yang Song, and Yuguang Fang, A formal study of trust-based routing in wireless ad hoc networks, In INFOCOM, 2010 Proceedings IEEE, pp. 1-9(2010).

[11] S. D. Khatawkar and N. Trivedi, Detection of gray hole in manet through cluster analysis, In 2015 2nd International Conference on Computing for Sustainable Global Development, pp.1752-1757(2015).

[12] Qualnet, Qualnet user manual, http://web.scalable-networks.com/content/qualnet (Online; accessed 9-Apr-2018]).