INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. (2014)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2837

Security and performance enhancement of AODV routing protocol

Harris Simaremare[1,2], Abdelhafid Abouaissa[1], Riri Fitri Sari[2] and Pascal Lorenz[1,*,†]

[1]*MIPS-GRTC laboratory, University of Haute Alsace, Colmar, France*
[2]*Network laboratory, Department of Electrical Engineering, Universitas Indonesia, Depok, Indonesia*

SUMMARY

A mobile ad hoc networks (MANET) is a decentralized, self-organizing, infrastructure-less network and adaptive gathering of independent mobile nodes. Because of the unique characteristics of MANET, the major issues to develop a routing protocol in MANET are the security aspect and the network performance. In this paper, we propose a new secure protocol called Trust *Ad Hoc* On-demand Distance Vector (AODV) using trust mechanism. Communication packets are only sent to the trusted neighbor nodes. Trust calculation is based on the behaviors and activities information of each node. It is divided in to trust global (TG) and trust local (TL). TG is a trust calculation based on the total of received routing packets and the total of sending routing packets. TL is a comparison between total received packets and total forwarded packets by neighbor node from specific nodes. Nodes conclude the total trust level of its neighbors by accumulating the TL and TG values. The performance of Trust AODV is evaluated under denial of service/distributed denial of service (DOS/DDOS) attack using network simulator NS-2. It is compared with the Trust Cross Layer Secure (TCLS) protocol. Simulation results show that the Trust AODV has a better performance than TCLS protocol in terms of end-to-end delay, packet delivery ratio, and overhead. Next, we improve the performance of Trust AODV using ant algorithm. The proposed protocol is called Trust AODV + Ant. The implementation of ant algorithm in the proposed secure protocol is by adding an ant agent to put the positive pheromone in the node if the node is trusted. Ant agent is represented as a routing packet. The pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. The path communication is selected based on the pheromone concentration and the shortest path. Trust AODV + Ant is compared with simple ant routing algorithm (SARA), AODV, and Trust AODV under DOS/DDOS attacks in terms of performance. Simulation results show that the packet delivery ratio and throughput of the Trust AODV increase after using ant algorithm. However, in terms of end-to-end delay, there is no significant improvement. Copyright © 2014 John Wiley & Sons, Ltd.

Received 12 May 2014; Revised 30 June 2014; Accepted 2 July 2014

KEY WORDS: AODV; ant algorithm; optimized protocol; performance; security; trust mechanism

1. INTRODUCTION

Currently, wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. The most used today is a wireless network built on top of a wired network. The main infrastructure requires a complex administrative work. This condition has limitations if the communications infrastructure is not available. The example is in the disaster areas or for military operations where it is not possible to build infrastructure quickly. This problem was solved by developing wireless *ad hoc* network mechanism, which is known as mobile *ad hoc* networks (MANET) [1–5].

A MANET is a decentralized, self-organizing, and infrastructure-less network. Every node acts as a router for establishing the communication between nodes over wireless links. Nodes forward

*Correspondence to: Pascal Lorenz, MIPS-GRTC laboratory, University of Haute Alsace, 34, Rue de Grillenbreit, 68000, Colmar, France.
†E-mail: lorenz@ieee.org

the communication packet between each other to find or establish the communication route [1–4]. In MANET, each node moves dynamically in an arbitrary manner, and every node can join or leave the network easily. It results a rapid change and unpredictable network topology.

There are two crucial issues and challenges due to the nature of MANET, that is, performance and security [3, 5, 6]. Routing protocol needs to have an optimal performance to improve the quality of communication, that is, communication delay, packet delivery ratio (PDR), throughput, and overhead. Routing protocol must have a minimum delay, maximum delivery ratio, and minimum overhead during the communication process. Several causes of the network performance degradation are external attack and rapid changing of the network topology.

A MANET has different personality and characteristics that surely trigger their own specific security concerns. Many potential attacks can be performed in each communication layers. MANET is more prone to physical threats than wired networks, and it promotes an environment for several attacks such as spoofing, eavesdropping, and denial of service (DoS) attacks. Most of these attacks are directed to the routing protocol schemes, and they tamper some of their activities taking advantage their insecure implementation and architecture. These well-known attacks are not executed directly, but they are prompted through the exploitation of the routing schemes, for instance, a DoS, a distributed DOS (DDoS), or a man-in-the-middle (MITM) attack. MITM is triggered and employed by MANET specific attacks such as blackhole and wormhole attacks [3, 6].

Based on these analyses, the routing protocol challenge in MANET is how to develop a robust security aware routing protocol that will eliminate the attacks existing in MANET without consuming the overall performance. In this paper, we propose a solution for routing protocol to cover the performance and security problem in MANET.

Security mechanism in MANET routing protocol is divided in two categories based on the security method, that is, cryptographic mechanism and trust-based mechanism. First, cryptographic mechanism. It will protect exchanging packet data, route discovery, and route maintenance process during the communication process. Many types of cryptography algorithms had been applied to secure the packet. Second is trust mechanism, which calculates a trust relationship between nodes before performing the communication process. Trust parameter nodes are represented by the level of trust. It is calculated from the network behavior. Secure routing protocol using trust mechanism has a better performance rather than using cryptography mechanism. We choose trust mechanism to improve the security aspect of protocol because our goal is to develop secure routing protocol with a good performance.

Many researchers proposed a modified Ad Hoc On-demand Distance Vector (AODV) routing protocol to increase the performance. Most of them modified the communication process or modified control packet to optimize AODV routing protocol. Not many researchers use bio-inspired algorithm to optimize this protocol. There are many varieties of bio-inspired algorithms such as ant colony optimization, evolutionary computation, genetic algorithms, iterated local search, simulated annealing, and tabu search [7].

Ant algorithm is most suitable to be implemented in MANET environments than other algorithms [8, 9]. By modeling an ant colony as a society of mobile agents, the biological ant's problem solving paradigm can be adopted to solve routing problems in a MANET. Some advantages and rationale of deploying ant colony optimization in *ad hoc* network routing are as follows: it can find an optimal path, autonomous, decentralized, fast adaptation, and multiple routes [9, 10]. Because of this reason, we use ant algorithm to improve the performance of the proposed secure protocol.

2. RELATED WORK

Many researchers have proposed a new mechanism to increase the security aspects of the AODV routing protocol. In this chapter, we will explore some of secure protocol using trust mechanism. Li *et al*. [11] calculate the trust opinion by using probability approach based on positive and negative events of each node. Positive events are the successful communication between two nodes, and negative events are the failed one. Trust calculation values are saved in the routing table of each node. Therefore, the nodes routing table needs to add a new field to save this information, which needs more memory allocation. On the other side, the mechanism needs to perform three steps of

DOI: 10.1002/dac

computation before sending the packets, that is, trust calculation procedure, trust combination procedure, and trust judging procedure. All of these steps increase delay of the communication process. Because the trust calculation is based on the communication behavior among the nodes, the trust calculation only obtain the value of communication behavior after the source node send data packets to the destination node. It means that the mechanism cannot detect the attack during the route discovery process.

Trust accumulation process has some problem about the proportional value of the trust opinion. The nodes that have direct connection between each other are more trusted to calculate the trust level of its neighbors than node that does not have a direct connection. Therefore, in the calculation of the trust accumulations, the node with direct connection should have a big proportion of value than the indirect node connection when calculating the total trust opinions. Raza *et al*. [12] proposed a trust accumulation opinion based on the connection condition among the nodes. The nodes with direct connection have a big proportion to conclude the total trust opinion values. Nodes with direct link have 90% of trust value, and the nodes with indirect link have only 10%.

With the different approach, Liu *et al*. [13] also proposed a trust opinion calculation based on the connection behaviors among the nodes. The total trust calculation is based in the important proportion of direct trust to the total trust. This mechanism also uses public key mechanism to encrypt the ID of the source node. This mechanism needs more resource to perform the cryptography mechanism and trust calculation. It also needs more memory allocations to save the trust information.

Trust calculation based on the level of successful packet exchanges is also used by Zhe *et al*. [14] to compute the trust level among the nodes. The proposed solution is more detail because not only based on routing packet exchanges, but also calculates the success ratio of the data packet. Total trust opinion is the accumulation of all trust calculation factors with a different proportion based on the link weight.

Rajaram *et al*. [15] proposed Trust Cross Layer Secure (TCLS) routing protocol. Security mechanisms in TCLS also use routing packet success ratio as a trust parameter. However, the success ratio is calculated based on the total route request (RREQ) arriving at the destination node, not the total RREQ between the neighbor nodes. Success ratio value will be added on the route reply (RREP) packet, and it is broadcasted to the next neighbor nodes. It is encrypted using cryptography method before being sent to the source node. If the intermediate node is failed to verify the digital signature of the destination node, then the RREP packet is dropped. The trust values of the node will be increased if the node has a high success ratio value, and the packet can be verified by the intermediate nodes.

Griffiths *et al*. [16] proposed Simple Trust Ad hoc On-demand Distance Vector (STAODV), which used acknowledgements as the single observable factor for assessing the success ratio of the routing packet. This mechanism is performed using promiscuous mode. Each time routing packets successfully arrive at the intermediate nodes, the trust level of the origin node that send the routing packet is increased. Trust level is decreased if the nodes do not appear to forward the routing packets. To detect whether a packet has been successfully forwarded, the packets that have been recently sent for forwarding are stored in the trust node data center. This data center needs some memory allocation to save all the information of the packet.

Bose *et al*. [17] proposed secure protocol using trust mechanism called efficient secure routing protocol. Trust has been established using signed acknowledgement based on asymmetric key cryptography. Key distribution problem is not cover by this mechanism. The mechanism will select one node admin as a minimal subset of all nodes that can form a fully connected network. It consists of all the administrators, which can reach out to all the neighbor nodes. This administrator node selection depends on symmetric link, node coverage, willingness of that node, and Trust.

Sharma *et al*. [18] propose the trust model to secure the AODV routing protocol. The trust calculation is divided into two, that is, trust combination algorithms and trust mapping functions. The routing table and the routing messages have been modified by adding the trust information. Trust information can be updated directly through monitoring in the neighborhood. The routing judgment based on the combination of each trust level calculation. In this way, the computation overhead can be largely reduced, and the trustworthiness of the routing procedure can be guaranteed as well. For a specific type of attack, Malekzadeh *et al*. [19] propose two distinct security models to

DOI: 10.1002/dac

prevent the DOS attacks. The models are capable of preventing the attacks by detecting and discarding the forgery control frames belonging to the attackers. In wireless networks, clear text form of control frames is a security flaw that can be exploited by the attackers. The proposed models improve the security performance of the wireless networks and enhance the network availability while maintaining the quality of the network performance. With different approach, Lacuesta R. *et al***.** in [20, 21] proposed the design of secure mechanism use computational cost based on the trust of the users and guarantee a secure protocol between the users and the mesh routers. This proposed mechanism use for secure the spontaneous network.

To improve the performance of MANET, Wu *et al*. [22] use an effective link lifetime estimation scheme. According to the current network topology and corresponding estimated link lifetime, the end-to-end connection is established adaptively in the best effort manner. Consequently, utilizing the network coding method, the relay node combines and forwards the packets on the working path. Furthermore, to keep the balance between the gain in reliability and the amount of redundant packets, the time for sending the redundant packets on the backup path is determined for the link stability intelligently.

Vaidya B. *et al*. [23] proposed a framework for secure voice transmission over multipath MANET. This secure framework modifies the route discovery phase by involving the establishment of secure multiple alternative paths between the source and destination nodes and the session key distribution mechanism.

Nakayama *et al*. in [24] proposed the new approach to detect the malicious node in *ad hoc* network. The new approach uses anomaly-detection scheme based on the dynamic learning process. This allows the training data to be updated at particular time intervals. The dynamic learning process involves calculating the projection distances based on multidimensional statistics using weighted coefficients and a forgetting curve. This scheme is more flexible to the new type of attack.

In other side, bio-inspired algorithm is also used to improve the performance of MANET. Gunes *et al.* [8] proposed a reactive protocol using ant algorithm called ant routing algorithm (ARA). Ant agent is represented as a control packet in routing process called forward ant (FANT) and backward ant (BANT). Both of these routing packets are used to establish and maintain the communication path. Each time FANT arrives at the intermediate node, it updates the node routing information and pheromone value.

Route discovery mechanism in ARA makes the overhead increases because the network is flooded by the FANT messages. Correia *et al*. [25] proposed the new protocol called simple ARA (SARA) to solve this problem. For controlling the FANT messages in the network, SARA uses Controlled Neighbor Broadcast (CNB) mechanism. With this mechanism, each node broadcasts the FANT to all of its neighbors and processes the packet, but only one of them broadcasts the FANT again to its own neighborhood. CNB uses probabilistic approach to decide the responsible node to rebroadcast the FANT messages to its neighborhood. When BANT messages arrive at source node, they provide multipath route to destination. Source node selects the route based on the paths cost link value. Similar with ARA protocol, the pheromone concentration increases if the FANT is successfully arrive at the intermediate node and the link is always used. In contrast, it decreases based on the life time when the link is not used.

The agents in Ant Colony routing algorithms communicate indirectly through the stigmergy and provide positive feedback to a solution by laying pheromone on the links. Moreover, they have negative feedback through evaporation and aging mechanisms, which avoids stagnation [26]. Zhang *et al*. [27] propose new mechanism to update the pheromone value. The pheromone trail is updated with two stages: in one stage, the first r iterative optimal solutions are employed to enhance search capability, and in another stage, only the iteration-best solution or the global-best solution is used to update pheromone. And besides that, the pheromone value is limited to an interval.

3. SECURITY ENHANCEMENT USING TRUST MECHANISM

Success ratio of received and sent packet becomes an important parameter to calculate the trust level of the nodes [14, 15]. Some of the proposed trust mechanism use the success ratio of routing packet or data packet or uses both of them. The aim of the trust calculation is to detect the potential attack and mitigate the attacker to avoid its impact to the network. The trust calculation can only perform

DOI: 10.1002/dac

after communication is established, if the data packet is used as a parameter. The attack cannot be detected by the trust mechanism if it is performed during the route discovery phases, because the nodes only calculate the success ratio of data packet. If the routing packet is used as a parameter to calculate the trust level, the trust mechanism directly starts the detection when the node performs the route discovery phases. This allows the trust mechanism to mitigate the attacker before the communication is established. In our trust calculation, we use routing packets as parameters to calculate the trust level of each node.

In [14], the success ratio is the comparison of the difference between success packet and failed packet to the accumulation of success packet and failed packet. In this approach, we cannot detect the detailed behaviors of each node. If the node is a malicious node, there is a possibility that the malicious nodes only send or forward some packets, not all the packets. However, in [15], the trust level of each node is calculated based on the comparison between total RREQ packet arrives in the destination node to the total of packets that have been forwarded by each node. This approach only uses the total number of RREQ packet that arrives in the destination. Each time the intermediate node forwards the routing packet, it will duplicate the routing packets based on the number of its neighbors. The total number of RREQ packet forwarded should be bigger than the total accepted RREQ in that node. With this approach, we assume that the total RREQ in the destination cannot be a parameter to calculate the trust level of each node in the network.

3.1. Proposed trust mechanism

Our proposed trust calculation computes the node trust level based on the behaviors and activities of each node. We activate the promiscuous mode to monitor the activities of each node. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. This mode of operation is sometimes given to a network snoop server that captures and saves all packets for analysis.

The assumptions about the normal activities are as follows:

- The node is a normal node if it forwards all the routing packet to its neighbors. Based on this assumption, the total number of sent packet must be equal or more than the total received packet at the nodes. The total forwarded RREQ depends on the total neighbors of that node.
- If the direct neighbor nodes do not receive the packet that has been forwarded by its neighbors, then this node is suspected as a malicious node.
- We assume that the network is running in promiscuous mode. With this mode, each node in the network could hear and capture all the activities of its neighbor [14]. Promiscuous allows a node to detect any transmitted packets, irrelevant of the actual destination that they are intended for [16].

Based on these assumptions, the trust behaviors calculation is divided into two kinds of trust, that is, trust local calculation (TL) and trust global calculations (TG). The definition of TL and TG is as follows.

- TG is the trust level calculation based on the total activities of the nodes. The activities are the comparison of the total received routing packets and the total of sent routing packets.
- TL is the node trust calculation based on the total number of routing packets that have been received from a specific node and forward it to its self.

Each node in the network will calculate the TL and TG of its neighbors. The node must accumulate TL and TG values to compute the total trust level of its neighbor nodes before sending or forwarding the packets. Equation (1) is used to calculate the TL, and Equation (2) is used to calculate the TG. In these equations, the node i wants to calculate the trust level of node j.

$$TL_{i,j} = \frac{\sum Pr_{i,j}}{\sum Pr_i \; f_{j,k}}; \; where \sum Pr_i \; f_{j,k} \neq 0 \tag{1}$$

$$TG_{i,j} = \frac{\sum Pr_j}{\sum Ps_j}; \quad where \quad \sum Ps_j \neq 0 \tag{2}$$

DOI: 10.1002/dac

Where $TL_{i,j}$ is the trust local opinion of node i to node j, $TG_{i,j}$ is the trust global opinion of node i to node j, Pr is the received routing packet, Ps_j is the sent routing packets, and $Pr_iF_{j,k}$ is the total forwarded routing packet from node i by the j that originates from node k.

Trust local is the comparison of routing packet from the specific nodes. It assesses the specific behaviors of each node. In AODV, the identical routing packet is received only once by the nodes. Because each time the node receives the routing packet, the packet ID will be checked. If the packet has been received before, then the latest one will be ignored. Based on this assumption, the node is a normal node if the TL calculation is equal to 1. Otherwise, the node is suspected as a malicious node. If the node is a trusted node, then the TL value is set to 1. Otherwise, the TL value is set to 0. TL opinion is set by using Equations (3) and (4).

$$TL_{i,j} = 1, \textit{ the node is trusted and the TL value is set to } 1 \tag{3}$$

$$TL_{i,j} \neq 1, \textit{ the node is untrusted and the TL value is set to } 0 \tag{4}$$

Trust global is the comparison between total routing packets that have been received and total routing packets that have been forwarded by the node. This indicates the global behaviors of the nodes. In the AODV protocol, routing packet will be forwarded if the intermediate node is not a destination node. The intermediate node forwards the routing packet to all its neighbors. Based on this condition, the total number of forwarded routing packet by the node is greater than the total of routing packet that has been received. Therefore, in the TG view, the node is a normal node if the TG calculation is equal to or more than 1. Otherwise, the node is suspected as a malicious node. If the node is a trusted node, then the TG value is set to 1. Otherwise, the TG value is set to 0. Equations (5) and (6) show the opinion of the TG calculation.

$$TG_{i,j} \leq 1, \textit{ the node is trusted and TG value is set to } 1 \tag{5}$$

$$TG_{i,j} \geq 1, \textit{ the node is untrusted and TG value is set to } 0 \tag{6}$$

Nodes conclude the total trust level of its neighbor by accumulating the TL and TG values. The node is marked as a trusted node when both result opinions accumulation of TL and TG are trusted. If one of the trust opinions is untrusted, the node is suspected as a malicious node. Based on this assumption, the conjunction logic (AND) is used to accumulate the trust opinion values. Equation (7) shows the accumulation model.

$$\textit{Total trust level}_{i,j} = TL_{i,j} \wedge TG_{i,j} \tag{7}$$

Trust mechanism calculation using TL and TG methods can be performed only if all the nodes in the network have the ability to hear all the activities of its neighbors. To fulfill this condition, the network must be in the promiscuous mode.

3.1.1. The destination sequence number (DSQ) value control mechanism. Each node monitors the destination sequence number (DSQ) value of RREP by calculating the difference in the routing table. When the node sends or forwards the RREQ packets, it records the destination address and the DSQ value in its routing table. When the node receives the RREP packets, it checks the routing table if there is a same destination address. If it does exist, the difference of DSQ is calculated. Otherwise, it forwards the RREP packets. The origin node of RREP is suspected as a malicious node if the DSQ difference value is more than threshold.

3.1.2. Route discovery phases. The initial condition of the all node in the network is considered as a trusted node. The default TL and TG values are 1. The source node broadcasts RREQ packet to all neighborhood for finding the communication route to the destination node. In the first time, source node found that all its neighbors are trusted nodes. Therefore, it sends the routing packet directly. When the intermediate node received the RREQ packet, it checks the trust level by calculating the TL and TG of the source node. If it is an untrusted node, then the RREQ is ignored. Otherwise,

DOI: 10.1002/dac

the intermediate node calculates the trust level of its next neighbor nodes and forwards the routing packet only to the trusted neighbor nodes. Trust calculation mechanism is performed in two sides, that is, at the sender node and the receiver node of routing packet.

Once the destination node receives RREQ packet, it generates and broadcasts the RREP packet to the source node through the reverse route that has been created by RREQ packet. During sending the RREP packet, the node does not need to recalculate the trust level of each node in its reverse path because it has been carried out when RREQ finds the path to destination. When the intermediate node receives RREP, it compares the DSQ value by performing the DSQ value control mechanism. When the source node receives RREP packet, it selects the route from the RREP with a normal DSQ value and the minimum number of hops. Figure 1 explains the route discovery procedures.

3.1.3. Route maintenance phases. When there is a broken link during the communication process, the nearest node to the broken link generates and sends the route error (RERR) messages to the source node. Once the source node receives the RERR messages, it re-initiates the route discovery phases if the communication is still needed.

4. PERFORMANCE IMPROVEMENT OF TRUST AD HOC ON-DEMAND DISTANCE VECTOR USING ANT ALGORITHM

The proposed optimize secure protocol is called Trust AODV + Ant. For implementing the ant algorithm in the Trust AODV, we add ant agent in the proposed protocol. The agent will find the path independently to the destination and deposit the positive pheromone into the routing table in every node in the path. Routing packet messages are used as an indicator to calculate the trust level of each node. The destination node generates and sends the RREP message to the source node after receiving the agent. The agent is represented as a routing packet. To measure the behavior of the node, every node monitors the activity of its neighbor when processing the RREQ, RREP, and RERR packet.

The positive pheromone is deposited into the routing table of the nodes only if the node is trusted based on the trust calculation. The agent updates the pheromone value by adding a constant number of using Equation (8) [20].

$$ph_{(u,j)} = ph_{(u,j)} + \alpha\ ,\ when\ \ TT_{u,j} = 1 \tag{8}$$

Where $ph_{(u,j)}$ is the pheromone value node u to j, $TT_{u,j}$ is the total trust level node u to j. $TT_{u,j}$ calculation uses Equation (7). When the path is never used, the pheromone concentration will be decreased based on the pheromone life time. The pheromone evaporation calculation is based on Equation (9).

4.0.1. Ant agent in Trust Ad Hoc On-demand Distance Vector. Ant agent in Trust AODV is represented as a routing packet. The structure of the packet agent is shown in Figure 2. The pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. The new routing table format is shown in Figure 3.

1. Source node broadcasts RREQ to all trusted neighbor nodes.
2. Initial condition for all node is trusted (TL=1 and TG =1)
3. Node received RREQ, it calculates TL and TG of the previous node
   a. If the previous node is untrusted, RREQ is ignored.
   b. If the previous node is trusted, node creates a reverse route to the origin node of the packet.
   c. Node calculates the TL and TG of the next neighbor nodes
   d. Node forwards the RREQ packet only to the trusted neighbor nodes.
4. Destination node receives RREQ packet, it generates and sends RREP to source node through the reverse route.
5. When the intermediate node receives RREP, it compares the DSQ values by performing the DSQ value control mechanism
6. Once the source node receives the RREP, it selects the communication route based on the normal DSQ value and the minimum number of hops.

Figure 1. Route discovery phases in Trust Ad Hoc On-demand Distance Vector.

DOI: 10.1002/dac

Agent Id
Source Id
Destination Id
Originator Id
Sequence number
Number of hop

Figure 2. Agent format in Trust Ad Hoc On-demand Distance Vector.

Destination ID	Seq Number	Next Hop	…..	Pheromone value

Figure 3. Format routing table.

4.0.2. Route discovery mechanism for ant agent. The source node broadcasts the agent after sending the RREQ packet to all neighbor nodes. The node calculates the trust level of its neighbor and sends the agent only to the trusted neighbor nodes. The number of agent in the network must be controlled to avoid the high overhead, congestion problem, and high energy consumptions. To control the number of agent in the network, we use CNB mechanism that is adopted from SARA protocol. In this mechanism, there is only one node that has the authority to rebroadcast the agent to its own neighborhood. It is selected by the source node using the probabilistic approach.

The source node calculates the TL and TG value of its neighbor before broadcasting the agent. Agent only broadcasts to the trusted neighbor nodes. After the intermediate node receives the agent, it checks the trust level of the origin node by calculating the TL and TG. If the origin node is trusted, it continues to process the agent. Otherwise, the agent is ignored. After all these steps, CNB procedures are performed as explained before for selecting the responsible node to forward the agent. Responsible node will calculate the trust level of its next neighbor nodes, and then only forward the packet to the trusted neighbors. This trust calculation process is always repeated at the sender and receiver node until the packet reaches the destination node. During these phases, agent deposits a positive pheromone in the routing table of the nodes if it is trusted and selected to forward the agent to the next node. The pheromone value is updated based on the Equation (8). Figure 4 describes the detail route discovery agent algorithm in our proposed protocol.

4.0.3. Route discovery phases in the proposed protocol. The route discovery phases are the procedure to find and establish the path communication to destination node. To find the route, source node broadcasts the RREQ packet to all neighbors. After that, source node continues to broadcast the agent to all neighbor following the route discovery agent procedures. The route discovery mechanism for the RREQ packet is similar with the standard route discovery mechanism in AODV protocol. When the destination node receives the RREQ packet, it checks the routing information whether the agent has arrived or not. If the destination node has received the agent, then it generates and broadcasts the RREP packet to the source node. The destination node only sends the RREP packet to the trusted node and node, which has a pheromone value equal to or more than 1. This information is provided in the routing table of each neighbor node. Otherwise, the

1. Source node calculates the TL and TG of its neighbors, and then broadcasts the agents only to the trusted neighbor.
2. The initial trust condition is trusted (trust value =1)
3. When the node receives the agent, it checks the trust value of the previous node.
   a. If the previous node is untrusted, then the agent is ignored.
   b. If the previous node is trusted, it performs the CNB mechanism
   c. Before forwarding the agents, it calculates the trust level of the next neighbor nodes. The packet is forwarded only to the trusted neighbor.
4. The destination node receives the agent. It generates and sends RREP to the source node after confirming that the RREQ has arrived in destination.

Figure 4. Route discovery phases for agent.

DOI: 10.1002/dac

destination node will wait to generate RREP until the agent arrives. Along the way to the source node, RREP will put the positive pheromones to every node in its path. Once the RREP reaches the source node, the path is established based on the pheromone value and the number of hops. Figure 5 describes the detailed procedure in the route discovery phases.

4.0.4. Route maintenance mechanism. Once the communication has been established between the source and the destination node, subsequent data packets are used to maintain the path. Evaporation mechanism is adopted from ARA to maintain the pheromone value. Pheromone value decreases when the link is not used, which is based on the life time of the pheromones. The pheromone calculation is shown in Equation (9) [8].

$$ph_{(u,j)} = (1 - q).\, ph_{(u,j)}\ ,\ where\ q \in (0, 1) \qquad 9$$

4.0.5. Route failure mechanism. The route failure mechanism is initiated when the broken link is detected during the communication. The route failure is detected through missing acknowledgement messages. This message is periodically sent by each node to indicate the link condition. If the broken link is detected, then the nearest node to the broken link sends RERR packet. When the node receives RERR message for a specific link, it deactivates the link by resetting the pheromone value to 0. When the pheromone value is 0, it means that the links are not used. After that, the node checks its routing table to find the alternative route. If exist, the communication is continue using this path. Otherwise, it sends an RERR to its neighbors, which will try to find other alternative route in its routing table. When the source node receives an RERR messages, it will re-initiate the route discovery phases if the communication is still needed.

5. ATTACKS SCENARIO AND PERFORMANCE METRIC

5.1. Attack scenario

(1) DOS/DDOS attacks

Denial of service attack will flood the victim nodes continuously with a useless request and in a big packet size. The victim cannot serve the real request to another node. The attacker node does not respond another packet routing from its neighbors, because it only floods the network with many request packets. All the direct neighbors can hear and calculate the trust level of the attacker node. Because the attacker node never forwards the packet, it is suspected as a malicious node, and it will be ignored from the communication process. Figure 6 describes the DOS attack.

(2) Blackhole attacks.

Attacker node will send the fake reply to indicate that it has a fresh route or it is a destination. Then source node will establish the communication with the attacker [5]. As a consequence, the real

1. The source node broadcasts RREQ to all neighbors.
2. After that, it broadcasts the packet agent using the route discovery agent procedures.
3. The agent updates the trusted node pheromone.
4. If node receives the RREQ, then it forwards the agents to the next node.
5. If the destination node receives the RREQ, it checks whether the packet agent has been received or not. If not, it waits until the agent arrives
6. If the agent has been received, the destination node generates and broadcasts RREP to the trusted node.
7. RREP will put the positive pheromones to every node in its path
8. Once the RREP arrives at the source, communication is started.
9. The source node selects the communication path based on the highest pheromone value.

Figure 5. Route discovery procedures.

DOI: 10.1002/dac

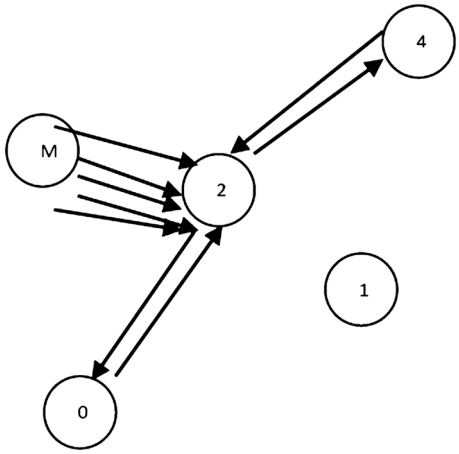

Figure 6. Denial of service attacks.

destination will never receive the packets because there is no established communication with the source node. Attacker node sends RREP packet with a higher DSQ to make the source node believe that it has a shortest path and a fresh path. Figure 7 describes the scenario of blackhole attack.

In AODV routing protocol, when the destination node receives a RREQ, it will generate and send route RREP packet. RREP packet consists of destination packet, source ID RREP, life time, and DSQ. We use DSQ value to detect the blackhole attack. Scenario in Figure 3 shows that node 0 wants to establish communication with node 4. During the route discovery process, the malicious node (M) sends RREP packet with a high DSQ value to indicate that it has a fresh route and it is a destination. In our trust mechanism, each node will compare the DSQ value of RREP. The origin node of RREP is suspected as a malicious node if the DSQ difference value is more than threshold. All the communication from the suspected node will be ignored.

5.2. Performance metric

(1) Packet delivery ratio is the ratio between the numbers of delivered data packet to destination against the number of packet sent. PDR reflects the network processing ability and data transferring ability, and as the main symbols of reliability, integrity, effectiveness, and correctness of the protocol. The protocol has a good performance if the PDR value is high. Equation (10) is utilized to calculate packet delivery ratio.

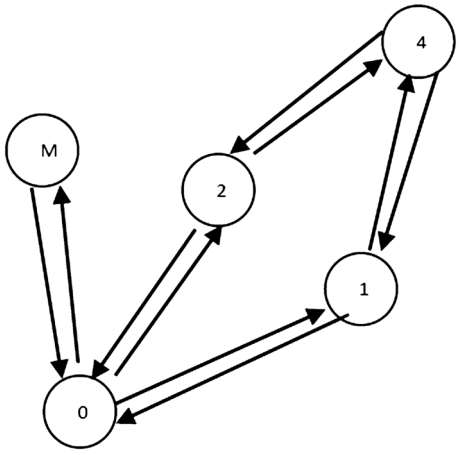

Figure 7. Blackhole attacks scenario.

DOI: 10.1002/dac

$$PDR = \frac{\sum Numbers\ of\ packet\ receive}{\sum Numbers\ of\ packet\ send} * 100\ \% \tag{10}$$

(2) End-to-end delay is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. Equation (11) is utilized to calculate the end-to-end delay.

$$End\ to\ end\ delay = \frac{\sum(arrive\ time - send\ time)}{\sum Number\ of\ link\ or\ connection} \tag{11}$$

(3) Routing overhead is equals to the ratio between the number of routing control packets transferred during the whole simulation process and the number of data packets. It refers to how many routing control packets are needed for one data packet transmission. Overhead is an important index that compares the performance among different routing protocols; moreover, it can evaluate the scalability of routing protocol, the network performance, and the energy consumption efficiency under lower bandwidth or congestion. Overhead calculates using Equation (12).

$$Routing\ overhead = \frac{\sum routing\ packet}{\sum packet\ received} \tag{12}$$

(4) Throughput is the average amount data received by the receiver per unit time. Equation (13) is utilized to calculate the throughput.

$$Throughput = \frac{\sum Size\ received\ packet}{\sum Stop\ time - start\ time} \tag{13}$$

6. SIMULATION AND RESULT ANALYSIS

6.1. Performance comparison of secure Trust Ad Hoc On-demand Distance Vector

Simulation has been conducted using NS-2 network simulator. DOS/DDOS and blackhole attacks are generated to evaluate the proposed protocol by increasing the number of attacks. There are seven nodes in the fixed position, that is, node 0, 1, 2, 3, 4, 5, and 6. The other nodes positions are set randomly. Simulation topology is shown in Figure 8. Table I shows the detailed simulation parameters. The simulation parameter values are selected according to the scenario and parameters of TCLS routing protocol [14].

In this simulation, the performance of Trust AODV is evaluated for the varying number of attackers moving in the same speed. The numbers of attackers are 5, 10, 15, 20, 25, and the speed

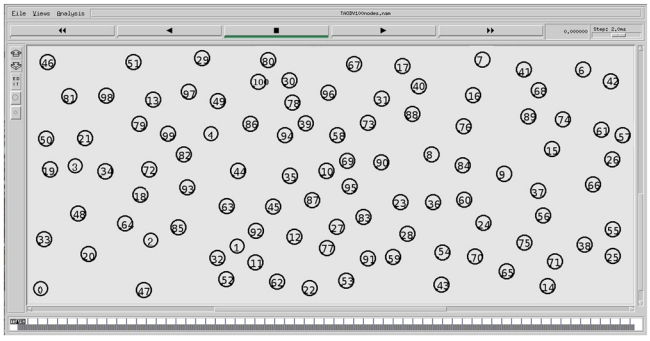

Figure 8. Simulation topology.

DOI: 10.1002/dac

Table I. Simulation parameters.

Parameters	Values
Simulation time	50 s
Topology	1000 m × 1000 m
Number of nodes	100
Speed s	30
Pause time	5 s
Traffic type	Constant Bit Rate (CBR)
Mobility model	Random way point
Packet size	512 bytes
Number of attacks	5,10,15,20,25

is 30 m/s. The variation number of attack is performed to evaluate its effect to the network performance.

Figure 9 shows the comparison of delay between Trust AODV and TCLS to the number of attacks when the speed is 30 m/s. Simulation results show that the trend of delay increases when the number of attacks in the network is increased. In the Trust AODV, the delay values are more stable with the small changes when the number of attacks is increased. This indicates that the trust mechanism can mitigate the attack before the communication route is established. The numbers of attacks do not give a significant effect to the delay values. However, in TCLS protocol, the delay value increases significantly when the number of attacks is increased. When there are many attackers in the network, the secure mechanism in TCLS needs more resource and time to process the security procedures such as trust calculation, verification using certificate, encryption, and decryption process to verify the packets. The Trust AODV has a better delay than the TCLS routing protocol.

Figure 10 shows the comparison of PDR between Trust AODV and TCLS to the number of attacks when the speed is 30 m/s. The simulation results show that the PDR of TCLS protocol decreases when the number of attacks is increased. This means that many packets cannot reach the destination. With the DOS attack, network will be flooded by the routing packets. Because routing packet size in TCLS is big, the possibility of collision and congestion in the network is high, which causes the increase of packet lost during the communication process. On the other hand, the security mechanism needs time to process the packet queue in each node. The packet queue in the node increases because the security mechanism needs time to verify it with cryptography mechanism.

In the Trust AODV, the PDR value is almost always stable (98%). The number of attacks does not affect to the PDR value. The trust mechanism can detect and mitigate the attack before the communication route is established. When the attacker is isolated from the network, the communication runs as a normal communication without attack. The Trust AODV has a better PDR than TCLS protocol.

Figure 11 shows the comparison of the overhead between Trust AODV and TCLS to the number of attacks when the speed is 30 m/s. Simulation results show the increasing trend of overhead when

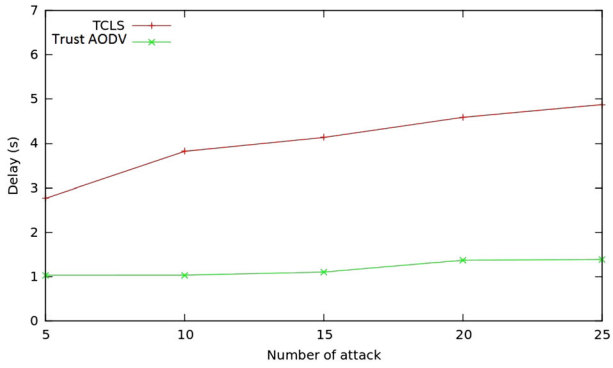

Figure 9. Comparison of delay to the number of attacks.

DOI: 10.1002/dac

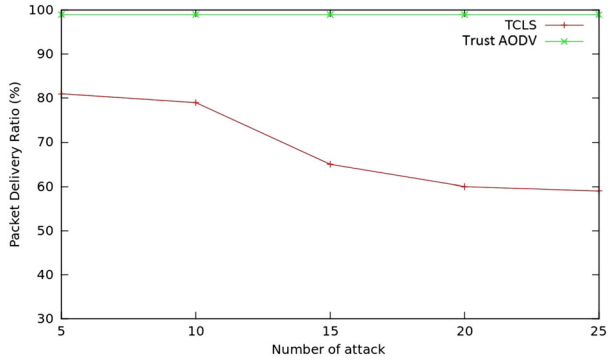

Figure 10. Comparison of packet delivery ratio to the number of attacks.

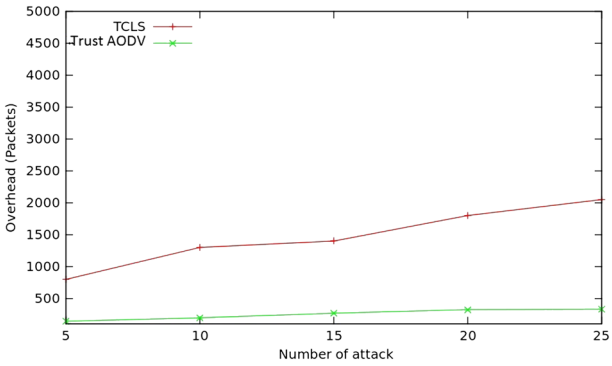

Figure 11. Comparison of overhead to the number of attacks.

the number of attack is increased. The number of packet that floods the network increases if there are many attackers in the network, which causes a high packet loss due to the network collision and network congestion. Trust AODV has a smaller overhead compared to TCLS due to the simple security mechanism in which no verification with cryptography process happens. In addition, the packet size of Trust AODV is not large.

Based on all of these simulation results, we can conclude that the Trust AODV has a better performance than TCLS protocol in terms of end-to-end delay, PDR, and overhead. Because the Trust AODV can detect and mitigate the attacker in the route discovery phases, the communication is performed as if it is a normal communication without attacks. In addition, the Trust AODV does not add any information in the routing table or in the routing packet header. Therefore, the packet size is similar with a normal packet in the AODV routing protocol.

6.2. Performance comparison secure Ad Hoc On-demand Distance Vector with ant algorithm

Trust AODV with ant algorithm is evaluated using NS-2 in terms of performance. The performance parameters are end-to-end delay, throughput, and PDR. The Trust AODV + Ant is compared with SARA, AODV, and Trust AODV. The aim is to prove that the ant algorithm can improve the performance of our proposed secure protocol. In this scenario, we only use DOS/DDOS attacks. The detail simulation parameter can be found in Table II. Each simulation scenario provides ten different values for delay, throughput, and PDR. We use statistical approach with standard deviation method to calculate the average value of each parameter. The confidence interval is 95%.

Figure 12 shows the comparison of the average end-to-end delay among Trust AODV + Ant, Trust AODV, SARA, and AODV to the varied number of nodes when the speed is 9 m/s under DOS/DDOS attacks. Simulation result shows that the average end-to-end delay of the protocol that uses trust mechanism is small. This means that the mechanism can maintain the communication during DOS/DDOS attack performs in the network. The difference of average delay between Trust

DOI: 10.1002/dac

Table II. Simulation parameters.

Parameter	Values
Simulation time	100 s
Topology	1000 m × 1000 m
Number of nodes	20, 30, 40, 50, 60, 70
Speed	9 m/s
Traffic type	Constant Bit Rate (CBR)
Mobility models	Random way point
Packet size	512 bytes
Pheromone life time	1 s

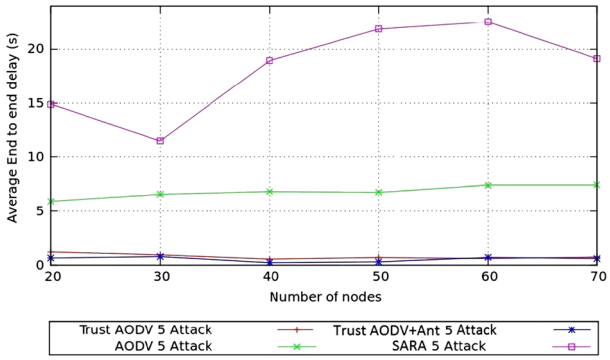

Figure 12. Average end-to-end delay versus number of nodes with speed 9 m/s.

AODV + Ant and Trust AODV is small. Based on these results, we can conclude that the implementation of ant algorithm in Trust AODV does not give a significant effect even when the number of nodes is increased.

The changes of the number of nodes in the network do not give a significant effect for the average end-to-end delay especially in the Trust AODV and the Trust AODV + Ant. The average end-to-end delay value is affected by the route discovery and route selection phases. In Trust AODV + Ant, each node should compute the trust level of its neighbors before broadcasting the agents. For the intermediate node, it calculates the trust of the previous node before processing the agents. Two sides trust calculation steps are similar with the Trust AODV mechanism. But in the Trust AODV + Ant, after the trust calculation is performed, the next step is the CNB calculation to choose the responsible node for forwarding the agents. These steps only create small difference the average end-to-end delay between both protocols. The ant algorithm implementation does not give a significant effect in terms of average end-to-end delay.

Figure 13 shows the effect of the number of nodes to the average PDR values in AODV, SARA, Trust AODV, and Trust AODV + Ant when the speed is 9 m/s under DOS/DDOS attacks. Simulation results show that the average PDR of the protocol with security mechanism is much higher compared to the protocol without security mechanism. Based on the graph, the average PDR of the Trust AODV + Ant is higher than the Trust AODV. For both protocols, the average PDR values increase when the number of nodes is increased. We can conclude that the performance of Trust AODV after using ant algorithm is better than before using ant algorithm. The average PDR value of the Trust AODV + Ant and the Trust AODV increases when the number on nodes in the networks is increased. The performance of Trust AODV + Ant is better than the Trust AODV in term of PDR. This due to the fact that ant algorithm can provide the multipath route between source and destination. When the number of node increases, the possibility to create the multipath route is big. With many alternative routes for establishing the communication, if there is a broken link during the communication process, the communication can still be continued using these alternative routes. The Trust AODV + Ant has a high average PDR than Trust AODV in the high speed mobility. The high speed mobility causes the possibility of broken link because of the rapid changes of

DOI: 10.1002/dac

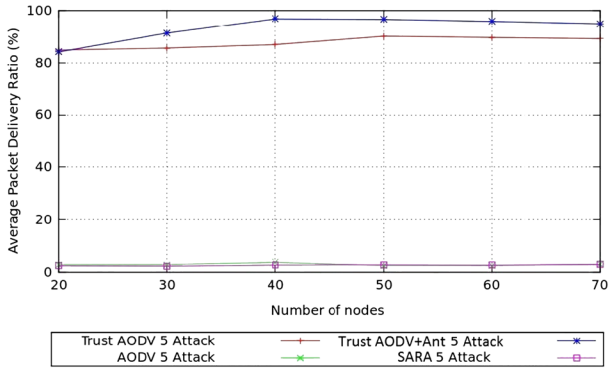

Figure 13. Average PDR vs number of nodes with the speed 9 m/s.

network topology that are big. The route failure mechanism in an ant algorithm can recover these problems and improve the performance in terms of the average PDR. On the other side, the CNB mechanism is running well to control the agent in the network. It can decrease the possibility of congestion in the communication process.

Figure 14 shows the effect of the number of nodes to the average throughput values in AODV, SARA, Trust AODV, and Trust AODV + Ant when the speed is 9 m/s under DOS/DDOS attacks. Simulation results show that the average throughput increases when the number of nodes is increased. The average throughput of Trust AODV + Ant is higher than Trust AODV. This means that the performance of Trust AODV after using ant algorithm is better than before using ant algorithm.

The average throughput of Trust AODV + Ant is better than other protocols. The possibility to create multipath route from the source to the destination increases when the number of node in the network is increased. Because the ant algorithm can provide the multipath route, the mechanism can cover the link failure problem and the average throughput increases. In an ant algorithm, the route selection mechanism is based on the pheromone concentration and the number of hops. The pheromone concentration indicates the quality of link. The possibility of packet that arrives at the destination node is big when the communication is performed through the link with a good quality.

There are no big differences of throughput value between the routing protocol without security mechanism (SARA and AODV) and the routing protocol with security mechanism (Trust AODV and Trust AODV + Ant). In the DOS/DDOS attack scenario, the attackers node sends request packet to the victims, so the victim will receive the packet in the high size. This makes the average throughput of SARA and AODV increases. In contrast, the PDR of SARA and AODV is small. The average throughput increases because the throughput parameter calculates the average amount data received by the receiver per unit time. However, the real source node cannot send the packet to the destination because of the victim that cannot serve the real request. That is why the PDR of SARA and AODV is small.

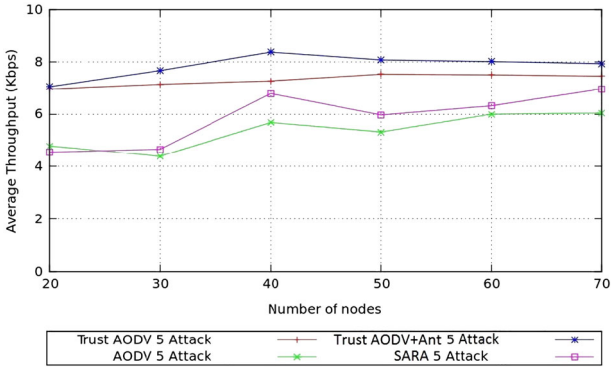

Figure 14. Average throughput versus number of nodes with speed 9 m/s.

DOI: 10.1002/dac

7. CONCLUSION AND FUTURE WORKS

In this paper, we propose a new trust mechanism to improve the security aspect of AODV routing protocol. Our trust mechanism calculates the trust level of each neighbor node before it sends the communications packet. Packet communications are only sent to the trusted neighbor nodes. Trust calculation is based on the behavior and activity information of each node. It is divided into TG and TL. Nodes conclude the total trust level of its neighbor by accumulating the TL and TG values. If one of the trust parameter is untrusted, the node is suspected as a malicious node.

The performance of the proposed protocol is evaluated under DOS/DDOS. It is compared with the similar type of secure AODV protocol, in this case TCLS protocol. Simulation results show that the Trust AODV has a better performance than TCLS protocol in terms of delay, PDR, and overhead.

We improve the performance of secure trust mechanism using ant algorithm. The proposed protocol called Trust AODV + Ant. The implementation of ant algorithm in the proposed secure protocol is by adding ant. Ant agent is represented as routing packet, and the pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. To control the number of agent in the network, we use CNB mechanism that is adopted from SARA protocol. In this mechanism, only one node has the authority to rebroadcast the agent to its own neighborhood.

Trust AODV + Ant is evaluated by using NS-2 in term of performance. The performance parameters are end-to-end delay, throughput, and PDR. This proposed protocol is compared with SARA, AODV, and Trust AODV under DOS/DDOS attacks. Simulation results show that the performance of proposed protocol increases when using ant algorithm in term of PDR and throughput. However, in terms of end-to-end delay, there is no significant effect to the performance.

In the future, there are some issues to improve our proposed secure mechanism. In the DSQ control mechanism, we will use automatic learning mechanism to define the threshold of difference DSQ value based on the network behaviors. In the pheromone calculations, we plan to improve the evaporation mechanism not only based on the time but also based on the local information in the node environments and network behaviors such as quality of link or other parameter.

ACKNOWLEDGEMENT

This research project is funded by The Directorate General of Higher Education Indonesia and Indonesian France Embassy.

REFERENCES

1. Abusalah L, Khokhar A, Guizani M. A survey of secure mobile ad hoc routing protocols. *IEEE Communications Surveys and Tutorials* 2008; **10**(4):78–93, DOI:10.1109/surv.2008.080407.
2. Marnerides A. Working with the gridkit overlay framework the secure-anthocnet overlay. PhD Thesis, Lancaster University 2007.
3. Yu X. A defense system on DDOS attacks in mobile ad hoc networks. PhD Thesis, Auburn University Alabama 2007.
4. Barritt BJ, Sheikh S, Al-Najjar C, Malakooti B. Mobile ad hoc network broadcasting: a multi-criteria approach. *International Journal of Communication Systems* 2011; **24**(4):438–460, DOI:10.1002/dac.1162.
5. Kannhavong B, Nakayama H, Nemoto Y, Kato N, Jamalipour A. A survey of routing attacks in mobile ad hoc networks, *IEEE Wireless Communications* 2007; **14**(5):85–91, DOI: 10.1109/MWC.2007.4396947.
6. Thanigaivel G, Kumar N, Yogesh P. Truncman: trust based routing mechanism using non-cooperative movement in mobile ad-hoc network. *Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP)*, 2012; 261–266, DOI:10.1109/DICTAP.2012.6215430.
7. Ahmed THAENA. Modeling and simulation of a routing protocol for ad hoc networks combining queuing network analysis and ant colony algorithms. PhD Thesis, University Duisburg-Essen, 2005.
8. Gunes M, Sorges U, Bouazizi I. ARA-the ant-colony based routing algorithm for MANETs. *Proceedings International Conference on Parallel Processing Workshops*, 2002; 79–85, DOI:10.1109/ICPPW.2002.1039715.
9. Li KH, Leu JS, Hoek J. Ant-based on-demand clustering routing protocol for mobile ad-hoc networks. *Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2013; 354–359, DOI:10.1109/IMIS.2013.66.

10. Ong DGC. Ant intelligence routing algorithm for mobile ad hoc networks. PhD Thesis, Malaysia University of Science and Technology 2004.
11. Li X, Lyu M, Liu J. A trust model based routing protocol for secure ad hoc networks. *Proceedings of the IEEE Aerospace Conference*, vol. **2**, 2004; 1286–1295, DOI:10.1109/AERO.2004.1367726.
12. Raza I, Hussain S. A trust based security framework for pure AODV network. International Conference on Information and Emerging Technologies, ICIET, 2007; 1–6, DOI:10.1109/ICIET.2007.4381316.
13. Liu Z, Lu S, Yan J. Secure routing protocol based trust for ad hoc networks. *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD*, vol. **1**, 2007; 279–283, DOI:10.1109/SNPD.2007.138.
14. Zhe L, Jun L, Dan L, Ye L. A security enhanced AODV routing protocol. In *Mobile Ad-hoc and Sensor Networks*, Lecture Notes in Computer Science, Jia X, Wu J, He Y (eds.). Springer: Berlin Heidelberg, vol. **3794**, 2005; 298–307, DOI:10.1007/11599463_30.
15. Rajaram A, Palaniswami S. A trust based cross layer security protocol for mobile Ad hoc networks. ArXiv e-prints Nov 2009.
16. Griffiths N, Jhumka A, Dawson A, Myers R. A simple trust model for on-demand routing in mobile ad-hoc networks. In *Intelligent Distributed Computing, Systems and Applications, Studies in Computational Intelligence*, Badica C, Mangioni G, Carchiolo V, Burdescu D (eds.). Springer: Berlin Heidelberg, vol. **162**, 2008; 105–114, DOI:10.1007/978-3-540-85257-5_11.
17. Bose D, Banerjee A, Bhattacharyya A, Saha H, Bhattacharyya D, Banerjee P. An efficient approach to secure routing in MANET. In *Advances in Computing and Information Technology, Advances in Intelligent Systems and Computing*, Meghanathan N, Nagamalai D, Chaki N (eds.). Springer: Berlin Heidelberg, vol. **176**, 2012; 765–776, DOI:10.1007/978-3-642-31513-8_78.
18. Pankaj S, Yogendra KJ. Trust based secure AODV in MANET. *Journal of Global Research in Computer Science* 2012; **13**(6).
19. Malekzadeh M, Ghani AAA, Subramaniam S. A new security model to prevent denial-of-service attacks and violation of availability in wireless networks. *International Journal of Communication Systems* 2012; **25**(7):903–925, DOI:10.1002/dac.1296.
20. Lacuesta R, Lloret J, Garcia M, Peñalver L. Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks. *Journal of Network and Computer Applications* 2011; **34**(2):492–505, DOI:10.1016/j.jnca.2010.03.024, ISSN: 1084-8045
21. Lacuesta R, Lloret J, Garcia M, Peñalver L. A secure protocol for spontaneous wireless ad hoc networks creation. *IEEE Transactions on Parallel and Distributed Systems* 2013; **24**(4):629–641, DOI:10.1109/TPDS.2012.168.
22. Wu D, Wang R, Zhen Y. Link stability-aware reliable packet transmitting mechanism in mobile ad hoc network. *International Journal of Communication Systems* 2012; **25**(12):1568–1584, DOI:10.1002/dac.1323.
23. Vaidya B, Denko MK, Rodrigues JJPC. Security mechanism for voice over multipath mobile *ad hoc* networks. *Wireless Communications and Mobile Computing* 2011; **11**(2):196–210, DOI:10.1002/wcm.948.
24. Nakayama H, Kurosawa S, Jamalipour A, Nemoto Y, Kato N. A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. *IEEE Transactions on Vehicular Technology* 2009; **58**(5):2471–2481, DOI:10.1109/TVT.2008.2010049.
25. Correia F, Vazo T. Simple ant routing algorithm strategies for a (multipurpose) {MANET} model. *Ad Hoc Networks* 2010; **8**(8):810–823, DOI:10.1016/j.adhoc.2010.03.003.
26. Singh G, Kumar N, Verma AK. Ant colony algorithms in MANETS: a review. *Journal of Network and Computer Applications* 2012; **35**(6):1964–1972, DOI:10.1016/j.jnca.2012.07.018.
27. Zhang Z, Feng Z. Two-stage updating pheromone for invariant ant colony optimization algorithm. *Expert Systems with Applications* 2012; **39**(1):706–712, DOI:10.1016/j.eswa.2011.07.062.