International Journal of Computer Science and Engineering (IJCSE)
ISSN 2278-9960
Vol. 2, Issue 4, Sep 2013, 1-8

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

ANT - APHID ROUTING ALGORITHM: A NEW TRUST BASED NATURE-INSPIRED ROUTING ALGORITHM

DIWAHAR S & SIVA SATHYA S

Department of Computer Science, Pondicherry University, Puducherry, Tamil Nadu, India

ABSTRACT

Mobile Ad-hoc Network (MANET) is a wireless communication network which does not rely on a pre-existing infrastructure or any centralized management. Security is a major concern in Mobile Ad hoc Network (MANET) because each node has to work cooperatively. This leads MANET to different forms of attacks from malicious nodes. Routing protocols are more vulnerable to various forms of attacks because any node can compromise the routing protocol functionality by disrupting the route discovery process. MANETs are vulnerable to various attacks from malicious node, the network works well only if the nodes are trustworthy and behave co-operatively. This paper presents a Bio-inspired solution to evaluate trustworthiness of the nodes, which is based on Ant-Aphid mutualism. This on-demand trust-based routing protocol for MANET is termed as Ant-Aphid based Routing for MANET to establish Security (ARMS).

KEYWORDS: Ant Colony, Bio-Inspired, MANET, Secure Routing, Trust

INTRODUCTION

A Mobile ad hoc networks (MANETs) is formed spontaneously by nodes coming together and forming a temporary network. There is no centralized control and its infrastructure-less nodes treat each other as routers to route packets along the network. Each node will communicate over wireless links and carry out the routing process maintaining the route in a self organised way. Due to MANETs characteristics like openness, protocol weakness and dynamic topology, they are unstable and exposed to different attacks. Routing is difficult in MANET because of its dynamic topology and paths initially effective becomes inefficient as the time progresses, Because of this routing information have to be updated at regular intervals.

MANETs are very flexible and suitable for applications like military and aerospace. So, security [1] plays a major role in MANET routing protocol. Nodes participating in routing take the decision to establish path between them, so trust establishment between nodes has greater importance for better security in MANET. So, establishing trust between nodes is very important in MANET. Trust based security is one way to improve security in MANET routing protocol [2][3][4]. Before participating in routing, nodes must have confidence that neighboring nodes are trustworthy. Each node's trustworthiness is based on previous experience with direct or indirect entity based on recommendation from other nodes. As in real life, trust levels are determined by particular actions that the trusted party can perform for trustee. Trust relationship between each node will help to take proper security measures and correct decision.

In this work, a new routing algorithm for MANET based on insects mutualism is proposed. For wired networks, there are few nature-inspired routing algorithms like (ABC [5] and AntNet [6]). They are proposed based on the ant colony optimization (ACO). The main idea of this work is to provide a trusted routing path continuously between nodes and to signify that the available path is more secure to forward packets. Ant based routing helps to find shortest path between nodes and aphids are used to provide a trust value to each node. Aphid produce the trust values as honeydew and ants collect the trust values and pass it to other nodes for comparing the other trust values. Ant based routing algorithm works in

a distributed way and provides automatic load balancing. In this paper, we propose a MANET routing algorithm, which works efficiently in finding the trusted path between nodes. The rest of the paper is organised as follows. Section 2 describes the related protocols in MANET, section 3 describes the proposed algorithm and section 4 illustrates the algorithm results.

RELATED WORK

Due to its specific challenges and applications in MANETs this well-liked research area has come up with a number of routing algorithms. Routing algorithm in MANETs are classified into two types: Proactive and Reactive. Proactive routing protocols (DSDV) continuously maintain the routing information between nodes. Topological and routing information are exchanged between nodes. Reactive protocols (AODV [8] and DSR [7]) establish a route between nodes only on demand. Routing and topological information are not exchanged among nodes.

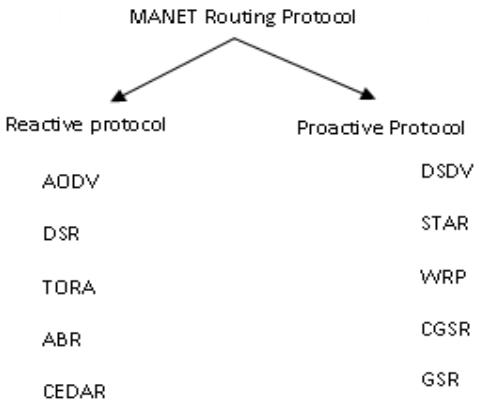

Figure 1: Taxonomy of MANET Routing Protocols

Reactive protocols are scalable and they construct a path only when they need to send packets to destination. This reduces the routing overhead, but can suffer oscillations in performance since they are never prepared for disrupting events. Most of these algorithms are single path. Multipath routing offers an alternative path in terms of link failure and load balancing. Problem with multipath is that optional paths are often infeasible by the time it is needed.

Trust based routing approaches can be used to assess the quality of information received and provide secure resource sharing. So, it is important to evaluate the trust value of nodes based on some metrics. *The definition of trust in MANETs point of view is given by [9]: A nodes trust is a subjective evaluation by an agent/ other neighbor node's trustworthiness and accuracy of information received when traversed through that node.* Each node's trustworthiness is calculated based on past experiences with direct or indirect entity based on recommendation from the neighboring nodes. Through the established trusted path in network, each node gets the trust values. Some of the trust based approaches [11] [12] [13] are given below:

- Fuzzy Logic Approach [10].
- Key Management [14].
- Subjective Logic.
- Graph Theory Approach etc.

The above mentioned approaches use different methods to calculate trust values among nodes. These approaches are used to calculate the trust values based on direct and recommended trust values from other nodes. Few approaches make use of packet forwarding ratio to calculate trust values among nodes. Trust calculation of each node is done in

different ways. Trust based approaches are calculated based on few factors, they are: encryption/decryption, updating trust value, authentication, and key management. Few ant based routing algorithms, are ABC [5], AntNet [6], and AntHocNet [10].

In these algorithms, the nodes send out routing agents in a regular interval to destination. The main function of these ant agents is to test the paths' quality and this information is used to update the routing table they pass. Routing tables contains the information about each destination and its neighbor, indicating the quality of path over the neighbor to its destination. The quality of path is called as pheromone value of the path. Pheromone information is used for both ants to route the packets. Ant based routing algorithm in MANET has several properties. They are highly adaptable to network changes, use active paths, provide multipath routing and load balancing.

PROPOSED ANT-APHID ALGORITHM

This work tries to exploit the relationship between the ant and aphids colony. Aphid is a kind of insect that lives in groups or colony and produce honey which is consumed by the ants and in turn the ants secure the aphid colony from external intruders. This is a kind of mutual relationship exhibited in nature. This mutualism between the ant and aphid colony is used in MANET to provide trust based secure routing. Here ant is used for routing the packets in the network and aphids that reside in each node produce honeydew. The amount of honey produced by them is taken as the trust value of the respective node. The packet structure used in AODV protocol is used here with some modification to carry the trust value between nodes. The algorithm could be described in two major steps:

- Trust Calculation.
- Route Determination.

Trust Calculation

The concept of trust in networks is derived from social science. One common definition of trust is, "Trust is the firm belief in the competence of an entity to act dependably, securely and reliably within a special context." The trust value is calculated based on past behaviour, present and future prediction. Subjective logic [15] [16] is used to calculate trust between nodes. Subjective logic calculates trust based on opinion. An opinion consists of belief, disbelief and uncertainty. A node may be uncertain about other node's trustworthiness because it does not collect enough evidences. Subjective logic provides a mapping method to represent trust between the evidence and opinion space.

In this work, we add two new fields in the routing table of each node: *events and opinion*.

- **Events**: It is used to known the successful communication between nodes. If it is success it will be entered as 1 and if it's not then it will be entered as 0.
- **Opinion** is the trust value of a neighbouring node as perceived or calculated by a given node.

A nodes opinion about others nodes are transmitted by "Hello" message to other nodes. The function of Aphids is to map the collected trust values (opinion) from other nodes. Mapping the nodes opinion is done through following equation:

$$\begin{cases} b_B^A = \dfrac{p}{p+n+2} \\ d_B^A = \dfrac{n}{p+n+2} \\ u_B^A = \dfrac{2}{p+n+2} \end{cases}, where\ u_B^A \neq 0 \quad (1)$$

Let $\omega^{A}_{B} = (b^{A}_{B}, d^{A}_{B}, u^{A}_{B})$ be node A's opinion about node B's trustworthiness in a MANET, and let p and n respectively be the positive and negative evidences collected by node A about node B's trustworthiness.

Combining the Trust Value

A nodes trust value is computed by direct and indirect trust values collected from other nodes. Collected trust values from other nodes are combined using two operators. They are (i). Discounting Operators and (ii) Consensus Operators.

Discounting Operators

Nodes combine two trust values (opinion). It is given by:

$$\begin{cases} b_C^{AB} = b_B^A b_C^B \\ d_C^{AB} = b_B^A d_C^B \\ u_C^{AB} = d_B^A + u_B^A + b_B^A u_c^b \end{cases} \quad (2)$$

ω^{AB}_{C} is called the discounting of ω^{B}_{C} by ω^{A}_{B} which expresses A's opinion about C as a result of B's advice to A. By using the symbol '$\otimes$' to designate this operator, we define $\omega^{AB}_{C} = \omega^{A}_{B} \otimes \omega^{B}_{C}$.

Consensus Operators

This operator is used to compare and combine the different opinion values about other nodes and arrive at a consensus. It is given by:

$$\begin{cases} b_C^{A,B} = \dfrac{b_C^A u_C^B + b_C^B u_C^A}{k} \\ d_C^{A,B} = \dfrac{d_C^A u_C^B + d_C^B u_C^A}{k} \\ u_C^{A,B} = \dfrac{u_C^A u_C^B}{k} \end{cases} \quad (3)$$

where $k = u^{A}_{C} + u^{B}_{C} - 2u^{A}_{C}u^{B}_{C}$ such that $k \neq 0$, Then $\omega^{A,B}_{C}$ is called the consensus between ω^{A}_{C} and ω^{B}_{C}, representing an imaginary node [A,B]'s opinion about C's trustworthiness, as if it represented both A and B. By using the symbol '$\oplus$' to designate this operator, we define $\omega^{A,B}_{C} = \omega^{A}_{C} \oplus \omega^{B}C$.

Route Determination

The second phase of the algorithm is route determination and it could be split into two micro steps:

- Routing Path Setup.
- Path Maintenance & Exploration.

Here, an ant is sent to find the shortest path to a destination and aphids residing in each node are used to calculate the trust value of the node. The trust value is calculated based on the honey dew content produced by the aphid colony in each node and subjective logic is used as said above. The value of trust is stored in each node's routing table thereby enabling the ants to know the trustworthiness of the nodes traversed by it. In discovering the routing path, a forward ant (FANT) is sent with RREQ message to know about other nodes in the network. Ant will collect the honeydew (trust value) from the node and carries it to the destination. In turn, the destination will look into the RREQ message and send back an ant (BANT) to source node with trusted routing path. In this secure path, the source forwards its packet to the destination. Thus this algorithm is used for providing a secure routing in MANET.

Routing Path Setup

When source node 'S' wants to start a communication session with destination d, it has to find a shortest trustworthy route. Initially it does not have routing & trust value information for d, hence it sends out FANTs to destination 'd' by broadcasting F_d to all nodes. The task of each F_d is to find a trustworthy path to destination from the source node. The routing & trust information of a node i is represented in its pheromone table T_t^i. This indicates the estimated goodness of going from I over neighbor n to destination d. If pheromone information is available, the ant will choose its next hop n with the probability $P_{nd.}$

$$P_{nd} = \frac{\left(T_{nd}^{i}\right)^2}{\sum_{i \in N_d}\left(T_{nd}^{i}\right)^2} + \omega_d^n \tag{4}$$

where ω_d^n - opinion of a node from other node and N_d – Neighbor of 'i' over a path 'd'.

If no pheromone information is available for d, the ant is broadcasted. Due to this broadcasting, ants can proliferate quickly over the network, following different paths to destination. Each destination ant keeps a trusted path (TP) of the node, it visited. At the destination, d it is converted to backward ants, which travel back to the source retracing T_P. The backward ant incrementally computes an estimate T_{TP} towards source, which is used to update the routing table. T_{tp} is the sum of local estimates $T_{i+1}{}^i$ in each node, where i ϵT_p is the time to reach next hop i+1.

$$T_{tp} = \sum_{i=1}^{n-1} T_{i+1}^{i} \tag{5}$$

In each intermediate node i $\epsilon T_{p,}$ the backward ant actually sets up a path towards the destination d, creating or updating the trust pheromone table entry $T_{Tnd}{}^i$ in T^i. If $T_d{}^i$ is the travelling time estimated by the ant, and n is the number of hops, the value $T_d{}^i$ is used to update the running average.

Path Maintenance and Exploration

Here, "HELLO" messages are used to guide the forward ant. These are short messages, broadcast in t_{hello} seconds by the nodes. If node receives a Hello messages from a node n for every t_{hello} seconds, it will be added in the routing table. If a node does not receive a Hello message in a particular time, that node will be removed from the routing table. This message is also used to detect broken links, which helps to clean up the information in the routing table.

The above algorithm is illustrated through the following steps:

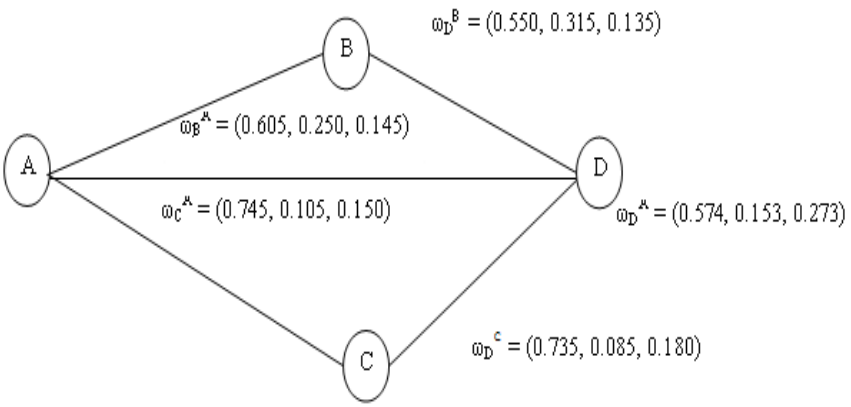

Figure 2: Illustration of the Algorithm

Consider the sample network shown in Figure 2

Step 1: When the network is initialised, each node is alien to another. Each node doesn't know about other node's behaviour.

Step 2: Each node send a "Hello" message to other nodes in the network. In hello message, each transmits its trust value of its neighboring nodes. This is computed based on the honeydew content in each node.

Step 3: On receiving hello message, node A picks a trust value of its neighbor and finds the trustworthy node by combining the other nodes trust value. At each node, opinion value about other node is displayed. Opinion consists of three values belief, disbelief and uncertainty.

Step 4: Now node A has three ways to reach destination D: one through B, one directly and other through C.

Step 5: Node A finds that the trust value of node C is higher when compared to other nodes in the network.

Step 6: So, node A forwards the packet to the destination through node C, which has high trust value than other nodes.

In this way, the proposed algorithm finds a secure routing path to forward the packet to destination.

SIMULATION ANALYSIS

The algorithm is simulated using QualNet and compared with AODV performance. QualNet is a discrete-event simulator developed by Scalable Networks. It is specially optimized for large scale MANETs. In this scenario nodes are placed at random in an area of 1500 x 400 m^2. Within this area, nodes move randomly to the chosen destination with chosen speed. The scenario's maximum speed is 20 m/s and the pause time is 35 seconds. Total time of the simulation is 1000 seconds. Source starts to transmit at a random time for a particular destination and sends it till the end. Transmission range is 350 meters and data rate is 2Mbit/s.

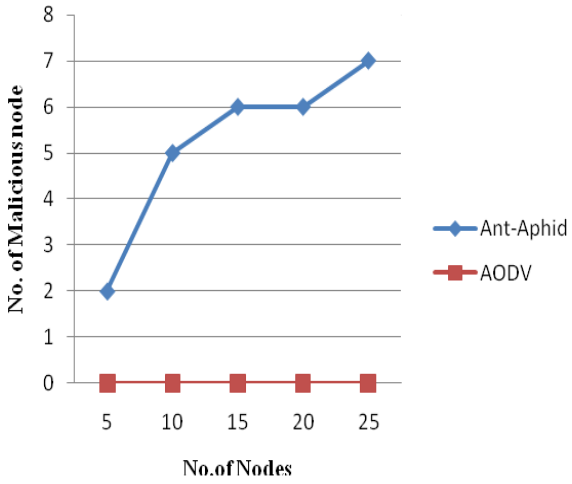

Figure 3: No. of Malicious Node versus No. of Nodes

The performance of the algorithm is evaluated based on the following metrics: Number of untrustworthy nodes isolated, packet delivery ratio and average delay. The algorithm isolates the malicious node from the network and strengthens the secure routing. From figure 3, we can see that our algorithm isolates a number of malicious nodes as it calculates the trust value of the node. When the number of nodes is increased, the algorithm detects more number of malicious nodes, whereas AODV doesn't have any mechanism to calculate the trust between nodes and it is difficult for it to find a malicious node.

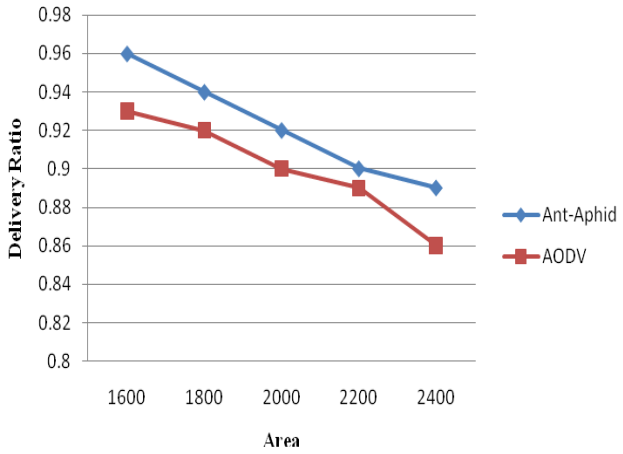

Figure 4: Delivery Ratio (Packets Arrive at Destination)

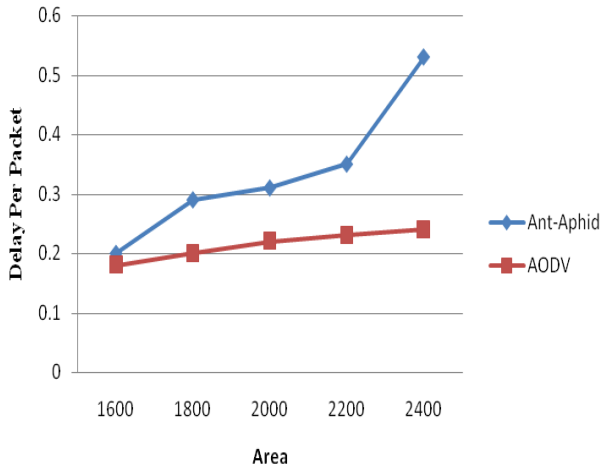

Figure 5: Delay per Packet

Figure 4 and 5 illustrates the packet delivery ratio at the destination. The proposed algorithm performs better then AODV in delivering the packets at destination. As we can see there is a decrease in AODV performance with area. Simulation results show that the proposed algorithm gives better delivery ratio than AODV in providing a secure routing path to destination. This is due to the construction of multi-path at route setup and alternative paths for route failures. This result in less packet loss. The Ant-Aphid algorithm has high average delay than AODV. As the scenarios size increases the average delay of AODV performs better. This is due to multi-path nature of the algorithm as it uses different paths to deliver the packets. Delivering the packets with low variability and maximum delay is an important factor in QoS routing.

CONCLUSIONS AND FUTURE WORK

The concept of insect mutualism for trust based routing using uncertain probability has been applied here. The trust between nodes is represented and calculated using *opinion*. After a logical analysis and simulation of the Ant-Aphid routing algorithm, it is concluded that our algorithm performs better than AODV and provides a better security for mobile ad hoc network. Our algorithm performs better in terms of delivery ratio, average delay and in finding the malicious nodes in the network. It provides a better security to the network by finding the malicious nodes and isolating them.

In future optimization of the routing algorithm would be carried out to test with existing secure routing protocol like ARAN and ARIADNE. We also like to apply our trust model into other applications (eg., key management) and other routing protocols of the MANETS (eg., DSR, DSDV etc.). A complete simulation evaluation will be conducted in terms of security analysis, message overhead and tolerance to mobile attackers.

REFERENCES

1. S. Corson and J.Macker. “Mobile ad hoc network (MANET): Routing protocol performance issues and evaluation considerations (rfc2501),” January 1999. http://www.ietf.org/rfc/rfc2501/txt .
2. Xiaoqi Li, Michael R. Lyu and Jiangchaun Liu, “A Trust Model Based Routing Protocol for Secure Ad Hoc Networks”, *Aerospace conference, 2004. Proceedings. 2004 IEEE pp. 1286-1295.*
3. Sanjay K. Dhurandher, Mohammad S. Obaidat, Karan Verma, Pushkar Gupta and Pravina Dhurandher, “FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems” *Journal of IEEE system, Vol. 5, No.2. pp 176-188, 2011.*
4. M. G. Zapata and N. Asokan “Securing ad hoc routing protocols” in *Proceedings of ACM Workshop on Wireless Security (WiSe ‘02)*. Atlanta, USA: ACM Press, September 2002. Pp.1-10.
5. R. Schoonderwoerd, O. Holland, J. Bruten, and L. Rothkrantz. “Ant-based load balancing in telecommunications networks”. *Adaptive Behavior*, (2):169{207, 1996.
6. G. Di Caro and M. Dorigo. AntNet: Distributed stigmergic control for communications networks. *Journal of Artificial Intelligence Research*, 9:317-365, 1998.
7. D. B Johnson and D. A. Maltz, “Dynamic Source Routing protocol in ad hoc wireless networks,” In T.lmielinski and H. Korth, editors, *Mobile Computing*, chapter 5, pages 153 – 181. Kluwer Acamedic publishers, Boston, USA, 1996.
8. C. Perkins, E. Royer, and S. Das, “Ad Hoc on Demand Distance Vector (AODV) Routing,” Jul. 2003, Internet experimental RFC 3561.
9. K. Govindan, P. Mohapatra, “Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey,” *IEEE Communications Surveys & Tutorials, VOL. 14, NO. 2, Second quarter, 2012*.
10. Hui Xia, Zhiping jia, Edwin H.-M. Sha, “Trust prediction and trust-based source routing in mobile ad hoc networks,” Journal of Ad Hoc Networks (2012).
11. M. G. Zapata and N. Asokan “Securing ad hoc routing protocols” in Proceedings of ACM Workshop on Wireless Security (WiSe ‘02). Atlanta, USA: ACM Press, September 2002. Pp.1-10,

    http://doi.acm.org/10.1145/570681.570682.
12. A.Josang, “A right type of trust for distributed systems”, Proceeding of 1996 workshop on security paradigms, 1996. Pp 119-131.
13. Xiaoqi Li, Michael R. Lyu and Jiangchaun Liu, “A trust model based routing protocol for secure ad hoc networks”, Aerospace conference, 2004. Proceedings. 2004 IEEE pp 1286-1295.
14. S. Neelakandan, J. Gokul Anand, “Trust based optimal routing in MANET’s,” Proceedings in ICETECT, 2011.
15. A. Josang, “A logic for uncertain probabilities,” *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol.9, no. 3, pp. 279-311, 2001.*
16. A. Josang, “A Subjective Metric for Authentication,” In *Proceedings of European Symposium on Research in Computer Security (ESORICS ‘98).* LNCS, Springer-verlag, 1998.