International Journal of Soft Computing 7 (3): 141-145, 2012
ISSN: 1816-9503

RRNN-AODV: A Reputation Routing Based on Nearest Neighbor in Mobile *ad hoc* Networks

[1]K. Tamizarasu and [2]M. Rajaram
[1]Department of CSE, Jayam College of Engineering and Technology,
Dharmapuri, Tamil Nadu, India
[2]Department of Electrical and Electronics Engineering,
Anna University of Technology, Tirunelveli, Tamil Nadu, India

Abstract: Packet forwarding presents a difficult challenge in Mobile *Ad hoc* Networks (MANETs) due to mobility, dynamic topology and lack of centralized management. Misbehavior due to selfishness or malice and lack of cooperation among nodes severely degrades the performance of the network. Most of the *ad hoc* routing protocol assumes that all the nodes are reliable and cooperative which is not true. Implementing security mechanisms including cryptographic techniques are overhead intensive and does not guarantee in performance improvement. In this study, an improved *Ad hoc* On-Demand Distance Vector (AODV), Nearest Neighbor Reputation (NNR) AODV is proposed. The focus in this research is to improve the performance of the network using reputation factors for route discovery. Another advantage of the proposed mechanism is enhanced security over the existing security mechanism.

Key words: Mobile *Ad hoc* Network (MANET), trust, reputation, *Ad hoc* On-Demand Distance Vector (AODV), NNR, India

INTRODUCTION

Trust and reputation (Gambetta, 1990; Josang *et al*., 2007) are principal components in many disciplines like sociology, economics and computer science. They have been extensively studied, discussed and many definitions have been proposed. In this study, researchers adopt the following definitions based on Mui *et al*. (2002).

Trust is a subjective expectation that a node has about another node's future behavior based on their encounter history. Reputation is a perception that nodes create through past actions about intentions and norms. Trust is viewed from a local perspective and is based on direct experience. Reputation, on the other hand is derived from:

- Direct encounters/observations
- Inferences based on indirectly gathered information (rating)

In a reputation system, nodes in the system rate the reputation of the other nodes and share it with other nodes. The three basic properties a reputation system must have to operate properly (Resnick *et al*., 2000) include:

- Nodes must live long so that every interaction raises expectation of future interactions
- Current interaction ratings are captured and distributed

Past interaction ratings should guide decisions about current interactions. An effective reputation system should fulfill requirements such as accurate rating, rating correctness, fast reaction to recent changes and robustness against attacks like liars and rating manipulations. MANET enhances security through awarding better reputation to nodes which have benign behavior. Better service is obtained for co-operative behavior of nodes with good reputation. Reputation systems are increasingly popular to secure online transactions. Such systems promote agents with good reputations as being better prospects for performing online transactions and are suitable for MANETs as nodes act trusting peer nodes to act benevolently. Such trust can be quantified through a reputation system. In MANET Systems, all nodes maintain reputation rating of its peers based on direct observation or recommendations from other nodes. Generally, the reputation systems work to promote benign behavior among nodes by offering better services in return for co-operative and benign

Corresponding Author: K. Tamizarasu, Department of CSE, Jayam College of Engineering and Technology, Dharmapuri, Tamil Nadu, India

behavior. Although, reputation systems are similar to payment systems, they are not economic in nature though, indirectly they may have monetary advantages. Nodes with good reputation gets the advantage of better service like forwarding of message earlier than nodes with lower reputation.

Most MANET trust management systems are reputation-based. Reputation-based classified as global reputation systems and local reputation system (Kamvar *et al*., 2003). In global reputation systems, each node knows the reputation value of other network nodes which in turn is achieved by exchanging an indirect reputation message over the network. CONFIDANT (Buchegger and Le Boudec, 2002) and CORE (Michiardi and Molva, 2002) are examples of global reputation system. In local reputation systems (Kamvar *et al*., 2003), each node keeps the reputation value of its neighboring nodes alone. Instead of distributing reputation value/information on a regular basis, the local reputation systems generally updates reputation values on its own observation. In reputation systems, each node receives feedback on what other nodes think of it. This mechanism can be either direct based on reputation table broadcasts as in the case of CONFIDANT or indirectly through observing positive recommendations of other nodes as in CORE. This could lead to a grunge war by nodes which get negative feedback about themselves.

AODV routing protocol (Perkins and Royer, 1999) provides a quick adaptation to dynamic link conditions, low processing and memory overhead and low network utilization. It keeps off problems (such as counting to infinity) associated with classical distance vector protocols. Its functionality is divided into: route discovery and route maintenance.

Route discovery: Route discovery is initiated when a source node broadcasts a Route Request (RREQ) for a route which does not exist for the chosen destination. At each hop, the RREQ creates a reverse route to source and on reaching destination or a intermediate node with route information, Route Reply (RREP) is generated. Unique destination sequence numbers are used in RREP to avoid routing loops and also indicate the route freshness. The intermediate nodes in route of RREP also update forward entries in routing tables. On receipt of RREP, source nodes start forwarding data.

Route maintenance: HELLO messages are the most common route maintenance message used for detecting and monitoring links to neighbors. Each node broadcasts periodic HELLO messages to neighbors for maintenance. On detection of a broken link either by a MAC layer acknowledgment or by non-receipt of HELLO messages, detecting nodes send Route Error (RERR) message to predecessors nodes that use broken links to reach their destinations. The RERR packet is sent to the source and the route is removed from the routing table.

Literature review: Samundiswary proposed an enhanced AODV by including trust based mechanism to improve security. Route trust and Node trust metrics were used by the trust mechanism to protect nodes from attacks. The proposed protocol chooses routes based on these trust metrics, thus avoiding the malicious nodes. The proposed protocol was implemented in a ZigBee Network Model. The experimental results showed that the proposed routing protocol achieves about 65% less overhead than the traditional AODV. The delivery ratio showed a marked improvement of 18-28% when compared to the standard AODV.

Boukerche proposed a novel distributed routing protocol SDAR by encrypting routing packet header and abstaining from using unreliable intermediate node. The protocols uses trustworthy intermediate nodes in the route without putting at risk of the anonymity of the communicating nodes, thus guarantying security, anonymity and high reliability of the established route. The proposed SDAR protocol had features like non-source based routing, no source control over route length and resilience against path hijacking.

Michiardi and Molva (2002) proposed CORE routing protocol which adopts the approach of reputation as a foundation of security mechanism to solve problems caused by misbehaving nodes in the network. In CORE nodes observe their neighbors or get information about the behavior of other nodes in the network from network members. Reputation is formed by combining information a node gets from its own experience and information that node gets from other nodes about a particular node of interest. A final reputation of a node is forme by a combination of three types of reputation; subjective reputation, indirect reputation and functional reputation.

CONFIDANT (Buchegger and Le Boudec, 2002) is an extension to the DSR protocol and it aims at detecting and isolating misbehaving nodes in order to discourage the uncooperative behavior of nodes during the routing process. It considers the changing behavior of nodes in the network at anytime. They adjust trust of nodes towards each other at every interaction. However, these two protocols have not considered nor distinguished

between malicious node behavior and problems caused by traffic congestion or benign link failures which are the most likely causes of routing failures in mobile *ad hoc* networks. Even if a failing node might be regarded as useless as malicious node but at least when a failing node recover from error it should not be regarded as harmful to communication of other nodes in the network.

In this study, it is proposed to incorporate an trust and reputation system to discover routes based on link quality and the node behaviour to improve the performance and overall security of the *ad hoc* network.

MATERIALS AND METHODS

The block diagram of the proposed reputation computation mechanism is shown in Fig. 1. Transmission success rate is represented as an exponentially smoothed moving average in link hysteresis. The hysteresis is calculated by iterative process and has a value between 0 and 1. The link quality is calculated after transmission of n packets as follows:

$$q_n = (1-h)\, q_{n-1} + h$$

Where:
q_n = The link quality
h = The hysteresis

Hysteresis threshold is defined and link with value above the threshold value is considered established link and with value below is dropped.

Expected Transmission count (ETX), computes the expected numbers of retransmissions required for a packet to move to and from a destination. The link quality is calculated based on the number of successful packets received by the node and its neighbour within a window period. The ETX is computed based on the link quality as follows:

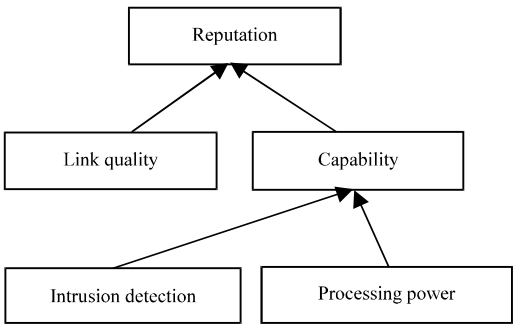

Fig. 1: Block diagram of the computation mechanism

$$ETX = \frac{1}{(LQ_X NLQ)}$$

Where:
LQ = The Link Quality
NLQ = The Neighbour Link Quality

ETX of the route is sum of all the ETX value of each hop in the route. When the value of ETX is 1, a perfect link is achieved. The performance metrics used to measure the link quality is given by:

$$p_{lq} = q_n \times ETX_{curr} - q_{n-1} \times ETX_{prev}$$

where, P_{lq} performance link quality. The reputation parameter is increased or decreased on the following conditions:

$$P_{lqcom} = \begin{bmatrix} 1 \text{ when } P_{lq} > 0 \\ 0 \text{ when } P_{lq} = 0 \\ -1 \text{ when } P_{lq} < 0 \end{bmatrix}$$

when, P_{lqcom} is a positive integer the behavior of the node can be identified as selfish or malicious using the following conditions:

$$R_{pr} = \frac{\text{Packets actually forwarded}}{\text{Total packets received for forwarding}}$$

The degree of trust on the node is increased or decreased on the following condition:

$$rel_{com} = \begin{bmatrix} 1 \text{ when } rel > 0.7 \\ -1 \text{ when } rel < 0.7 \end{bmatrix}$$

The capability of the node is computed using the relationship:

$$C = \sum x_i / N$$

Where:
x_1 = The presence of anti virus
x_2 = The presence of IDS
x_3 = The presence of fire wall

The reputation of the Node A with respect to Node B is given by:

$$R_{A-B} = P_{lq} + rel_{com} + C$$

The Hello message of the AODV is modified and shown in Fig. 2. The reply message from the nodes within one hop destination to the node initiating the modified

1	J	R	G	D	U	Reserved	0
RREQ ID							
Destination IP address							
Destination sequence number							
Originator IP address							
Originator sequence number							
1	Len	Pla	rel	c			

Fig. 2: The modified Hello message

Type	R	A	Reserved	Prefix Sz	Hop count
Destination IP address					
Destination sequence number					
Originator IP address					
Lifetime					
1	Len	Pla	rel	c	

Fig. 3: The reply sent for the modified Hello message

Hello message is shown in Fig. 3. During route discovery from source to destination the optimal route is selected by using the metric of R.

RESULTS AND DISCUSSION

The proposed method was simulated using OPNET. 25 nodes with random mobility covering an area of 5 km^2 was used in the simulation setup. Two experiments were conducted with the same setup with the first setup using AODV routing protocol and the second setup with the proposed routing protocol. The throughput obtained for random traffic sent between the nodes is shown in Fig. 4. Establishing route with reputation based nodes where link quality plays a crucial role is seen in the improved throughput. The number of hops to reach destination globally is shown in Fig. 5

From Fig. 5, it is seen that the average number of hops increase by one when compared to regular AODV. However, from Fig. 4 it is seen that the throughput increases once the route is established. The overall route discovery time is shown in Fig. 6. Figure 7 shows the media access delay.

The proposed method reduces the media access delay compared to AODV. The increased route discovery time can be attributed to the selection of the route based on reputation metrics and not on minimum number of hops.

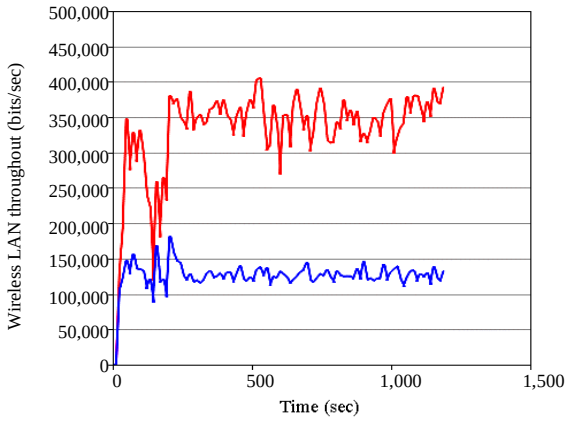

Fig. 4: The throughput of the proposed system and AODV

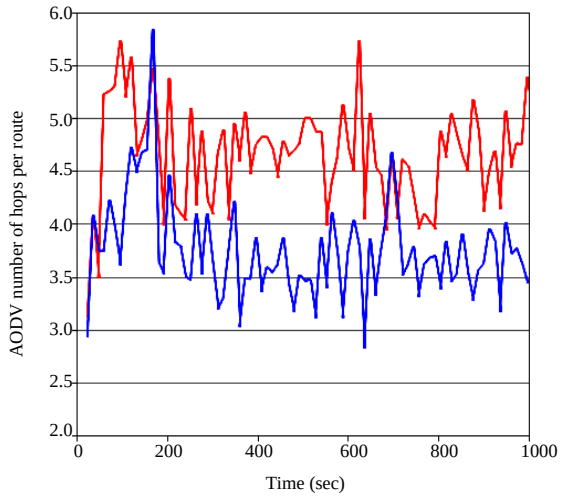

Fig. 5: The number of hops to reach destination

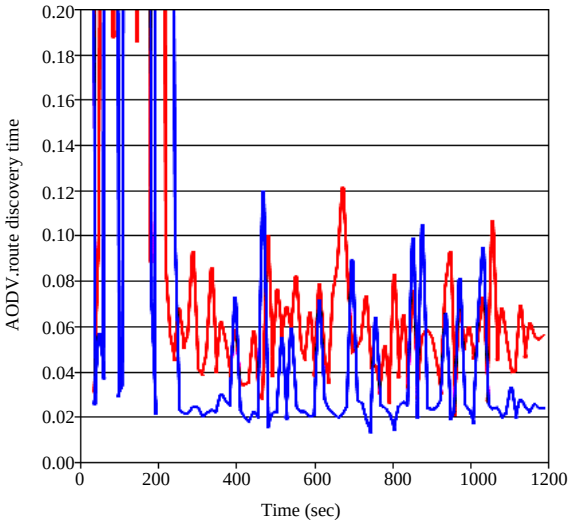

Fig. 6: The route discovery time

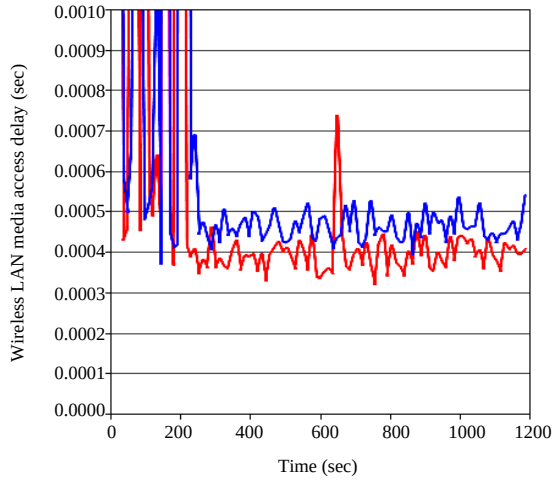

Fig. 7: The media access delay

CONCLUSION

In this study, an improved AODV routing protocol was proposed to improve the network performance. The proposed method combines trust and link quality for computation of reputation of nodes. A novel reputation computation mechanism was proposed and implemented. Simulations were carried out for 1000 sec and compared with AODV. The throughput of the proposed system improves along with the media access delay. However, the route discovery time is substantially higher. Further research needs to be done to see the performance of the proposed method with large number of nodes.

REFERENCES

Buchegger, S. and J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile *Ad hoc* Networking and Computing, June 9-11, 2002, Lausanne, Switzerland, pp: 226-236.

Gambetta, D., 1990. Can We Trust Trust? In: Trust Making and Breaking Cooperative Relations, Gambetta, D. (Ed.). Blackwell, Oxford, UK., pp: 213-237.

Josang, A., R. Ismail and C. Boyd, 2007. A survey of trust and reputation systems for online service provision. Decision Support Syst., 43: 618-644.

Kamvar, S.D., M. T. Schlosser and H. Garcia-Molina, 2003. The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th International Conference on World Wide Web, May 20-24, 2003, Budapest, Hungary, pp: 640-651.

Michiardi, P. and R. Molva, 2002. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile *ad hoc* networks. Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, September 26-27, 2002, Portoroz, Slovenia, pp: 107-121.

Mui, L., M. Mohtsahemi and A. Halberstadt, 2002. A computational model of trust and reputation. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, January 7-10, 2002, Hawaii, USA., pp: 2431-2439.

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 25-26, 1999, New Orleans, LA., pp: 90-100.

Resnick, P., K. Kuwabara, R. Zeckhauser and E. Friedman, 2000. Reputation systems. Commun. ACM, 43: 45-48.