Trust based Energy aware Reactive Routing Protocol for Wireless Sensor Networks

P.Samundiswary
Assistant Professor
Dept. of Electronics Engineering
Pondicherry University
Pondicherry, INDIA

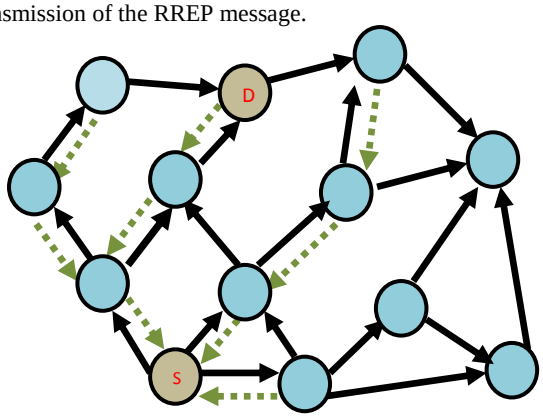
ABSTRACT
Recently, Wireless Sensor Networks (WSNs) have drawn a lot of attention due to broad applications in military, civilian wildlife monitoring and disaster management. Sensor networks are composed of large number of densely deployed sensor nodes with limited energy and computation. Since these nodes operate in a physically insecure environment, they are susceptible to various types of attacks. These attacks infuse malevolent packets by compromising the nodes. Various secured reactive routing protocols have been developed with the help of cryptographic techniques in order to protect the network against the compromised nodes. However the routing protocols using encryption schemes require large memory for storing the keys and more computation. Further, these protocols have been developed without the consideration of energy aware algorithm. In this paper, trust based energy aware reactive routing protocol is developed for wireless sensor networks by appending trust based mechanism in the energy aware reactive routing protocol. The performance of the proposed protocol has been evaluated and analysed in terms of delivery ratio for different number of nodes.

Keywords
WSN, AODV, RREQ, RREP, EAODV, ATV, OTV, TEAODV.

1. INTRODUCTION
Recent advances in wireless and ubiquitous computing have prompted much research attention in the area of WSN. Security is identified to be the most challenging research issue in sensor networks and also security plays an important role in WSNs since the nodes of these types of networks are deployed in hostile environment [1]. Due to the small size and unattended deployment of nodes, the attackers can easily capture and convert them as malicious nodes. In order to safeguard the networks from the compromised nodes, several routing protocols have been developed by using link layer encryption techniques. But, requirements of such secure routing protocols include configuration of the nodes with encryption keys [2] and the creation of a centralized or distributed key repository to realize different security services in the network. In addition, secure routing protocols utilising cryptographic methods also require excessive overheads [3, 4]. Instead, trust based security scheme is used to defend the nodes of wireless sensor networks against malicious nodes. Trust based protocols locate trusted route rather than secure route and their models are influenced by human behaviour models [5], [6]. However, trust based routing protocols will not utilize the energy aware algorithm. Hence, trust based energy aware reacting routing protocol is proposed by incorporating trust based security technique in energy aware reactive routing protocol which is described in this paper. The paper is organized as follows: Section 2 describes about the ad hoc on demand distance vector routing protocol. Energy aware ad hoc on demand distance vector (reactive type) routing protocol is explained in section 3. Section 4 deals with the proposed trust based energy aware reactive routing protocol of wireless sensor networks. Simulation results are discussed in Section 5 to obtain delivery ratio of the proposed security scheme and conclusions are drawn in Section 6.

2. AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL
AODV is a reactive routing protocol which accomplishes the route discovery whenever a data transfer is requested between nodes. The AODV routing protocol is also known as on demand protocol since it searches a new route only by request of source node. It uses traditional routing tables, one route entry per destination and Destination Sequence Number (DSN) to ensure the freshness of routes and avoid the routing loops [7]. This will greatly increase the efficiency of routing processes. The protocol forwards the packet by using two routing phases. They are i) route discovery and ii) route maintenance

2.1 Route Discovery
Route discovery is initiated when a source node request a route to a new destination or when the lifetime of an existing route to the destination has expired [8]. The process is initiated by flooding the RREQ messages as shown in Figure 1. The source node broadcasts a RREQ packet to its neighbours until the required route is discovered. When a neighbour node receives a RREQ, it checks whether the sought route is a 'fresh enough' route using its DSN. If the DSN of the sought route is greater than DSN of RREQ, the route is said to be a 'fresh enough' route. At the same time, the neighbouring node or destination node replies with a RREP packet to the source node. The RREP is traveled through the reverse path noted by each node during the transmission of RREQ [9]. Then the source node establishes the forward path for the data transmission during the transmission of the RREP message.



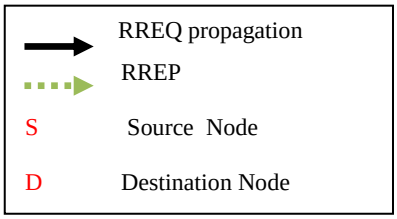


Figure 1: Flooding of RREQ messages

2.2 Route Maintenance

To maintain connectivity, nodes either periodically broadcast HELLO packets to their neighbours or use acknowledgement based mechanisms at the link or network layers. Upon detecting a link break, a node could choose to repair the link locally (if the destination is no farther than MAX_REPAIR_TTL hops away) or send a RERR packet to notify its upstream nodes. A RERR message contains the list of those destinations which are not reachable due to the loss of connectivity.

The AODV routing protocol determines a least hop-count path between the source and the destination, thus minimizing the end-to-end delay of data transfer. However, if two nodes perform data transfer by using the specific path for long time, nodes belonging in this path consume more battery power than other nodes, resulting in earlier draining of battery power of nodes involved in the routing [10]. The increase of power-exhausted nodes creates partitions in the wireless sensor network. Hence the lifetime of the network is reduced and the network performance will be degraded without considering the energy consumption of the nodes in the routing process.

3. ENERGY AWARE AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

To enhance the performance of network, EAODV protocol is developed by considering the residual energy of sensor nodes which is included in the RREQ packet along with the hop count for the transmission of packets from source to destination node in the ad hoc on demand distance vector routing protocol.

The optimum route is determined by using the value of parameter α described in equation 1.

$$\alpha = \frac{Min - RE}{k.No - Hops} \quad \ldots\ldots\ldots\ldots(1)$$

where

Min-RE is the minimum residual energy on the route
No-Hops is the hop count of the route between source and destination
k is the weight cofficients for the hop count

The destination node calculates the values of α for received routes and selects a route that has the largest value of α. Then the EAODV protocol collects routes that have the minimum residual energy of nodes relatively large and have the least hop-count, and then determines a proper route among them, which consumes the minimum network energy compared to any other routes [11].

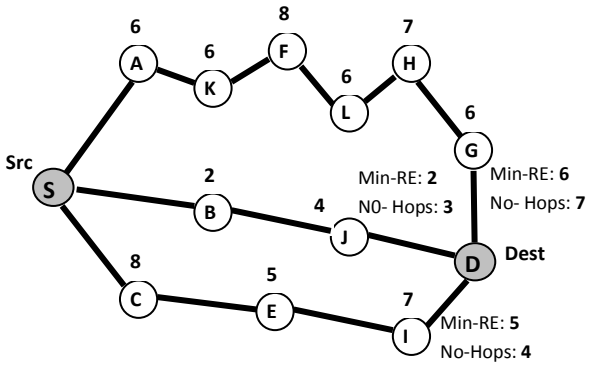


Figure 2. Schematic diagram representing EAODV protocol

The operation of EAODV routing protocol is explained with the help of two routes as illustrated in Figure 2. Here a simple routing is considered from source node S to destination node D. The number written on a node represents the value of residual node energy. Since the route 1 considers only the minimum hop count, it selects route <S-B-J-D> which has the hop count of 3. In route 2, data is transferred from source to destination node by choosing the route <S-C-E-I-D> which has largest α value of 1.25. Route 1 selects the shortest path without considering residual energy of nodes, which is the same as the AODV routing algorithm. Route 2 improves the drawbacks of Route 1 by considering both residual energy and hop count. It improves the lifetime of network by making almost all nodes to involve in data transfer

4. TRUST BASED ENERGY AWARE AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The enhanced version of trust based ad hoc on demand distance vector routing protocol [12-14] available for adhoc networks and WSN is implemented in the energy aware reactive routing protocol for different number of nodes and malicious nodes. There are two trust values associated with the Trust based Energy aware Ad hoc On demand Distance Vector (TEAODV) protocol. They are route trust and node trust. Route trust is computed by every node for each route in its routing table. The route trust is a measure of the reliability with which a packet can reach the destination, if forwarded by the node on that particular route. Route trust is calculated as a ratio of the number of packets received at destination D to the number of packets forwarded by the node under consideration (from S to D on that route). Node trust is computed based on the difference between the nodes' Advertised route Trust Value (ATV) to the destination and the Observed Trust Value (OTV) computed for the current data transfer. Node trust is incorporated in the neighbour trust table which is maintained by every node to obtain the trust value of neighbhour node.

The node trust is identified in the following procedure. When a node 'i' forwards or generates a RREP, i advertise its trust on the route under consideration to its immediate upstream node P. Node P caches this route trust value as ATV of node i on that route and compares it with the OTV. The node 'i' receives an incentive if the OTV is within an admissible range of ATV. Then the node P allows the node i to forward the packets. This indicates the absence of compromised nodes. Otherwise, the node i is penalized, i.e., node P isolates the

node i by not forwarding the packets and not entertaining any RREQs which indicates that the node is identified as malicious node. Then the node P finds alternate node to transmit the packet to the destination. Further, the route selection criterion is based on Route Selection Value (RSV). In this scheme, a source node calculates the RSV for all its available routes to the destination and it finally chooses the route which has the highest RSV. If two routes have the same RSV then the following norms are used to break the tie. The first condition is that the routes with highest route trust are selected. The second criterion is that if the routes have same route trust values then the route with the highest immediate downstream neighbours' node trust (as perceived by the source/immediate upstream node) is chosen. The third one is that if the immediate downstream neighbours' node trust is also the same, then the shortest route is chosen. . The process is repeated until all the packets reach the destination from the source node within the assumed simulation time. Hence, in TEAODV, data is transferred from source to destination node by selecting the path having node trust and route trust in addition with minimum energy consumption and shortest path.

5. SIMULATION RESULTS AND DISCUSSION

The trust based mechanism is appended in EAODV to obtain the TEAODV protocol. TEAODV is simulated by using ns-2.32 [15]. The performance parameter namely delivery ratio is calculated for 150 nodes and 200 nodes by varying the malicious nodes from 5 to 30 with the coverage area of 500×500m^2.The parameters used in the simulation are listed in Table 1.

Table 1: Simulation Parameters

Simulation parameters	Values
Number of nodes	150 , 200
Geographical area(m^2)	500×500
Number of malicious nodes	5 to 30
Traffic Type	CBR
Mobility model	Random way point
Simulation time(s)	100

5.1 Delivery Ratio for 150 Nodes

Delivery ratio analysis is studied by varying the malicious nodes for 150 nodes by considering the coverage area of 500×500m^2. It is observed through the simulation result illustrated in Figure 3 that the delivery ratio of TEAODV is higher than that of EAODV protocol by 10%-15% approximately. The improvement in the delivery ratio is due to the fact that TEAODV improves the forwarding rate by using trusted path along with the path having minimum energy level and less hop count for transmitting the packets from the source to destination node

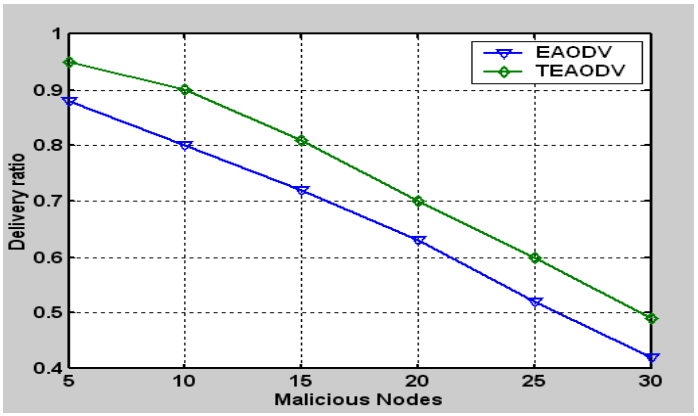


Figure 3. Delivery ratio with respect to no. of malicious nodes for 150 nodes with coverage area 500×500(m^2)

5.2 Delivery Ratio for 200 Nodes

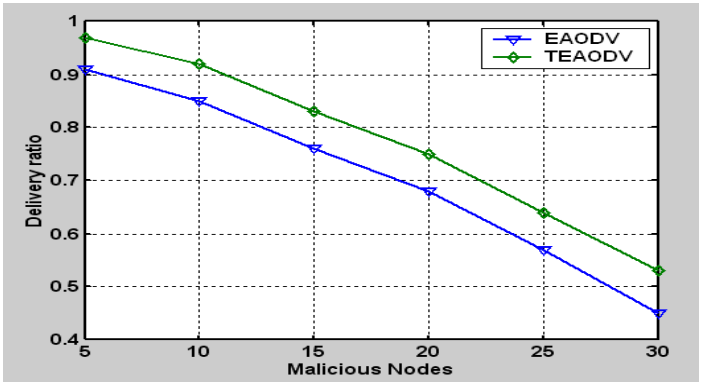


Figure 4. Delivery ratio with respect to no. of malicious nodes for 200 nodes with coverage area 500×500(m^2)

Delivery ratio performance is examined for 200 nodes by varying the malicious nodes from 5 to 30 with the coverage area of 500×500m^2. Simulation result shown in Figure 4 demonstrates that TEAODV outperforms EAODV by achieving higher delivery ratio of approximately 17% considering the malicious nodes of value 30. The reason is due to the usage of trusted route and node trust by TEAODV to improve the forwarding rate of packets.

6. CONCLUSION

TEAODV protocol is implemented for mobile sensor network with the help of ns-2.32 simulator. Routing performance namely delivery ratio of TEAODV is determined and also compared with EAODV protocol by varying the malicious nodes from 5 to 30 for 150 and 200 nodes with coverage area of 500×500 m^2. The results show that an improvement of approximately 13 % in delivery ratio is achieved by using the TEAODV protocol than the EAODV. This is mainly due to the successful transmission of packets from source to destination nodes by considering trusted path along with path having minimum energy level nodes and shortest route.

7. REFERENCES

[1]. C.Karlof and D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, Anchorage, AK, pp.113-127, May 2003.

[2] A.Perrig, J.Stankovic and D.Wagner, "Security in wireless sensor networks", *Communications of the ACM*, vol. 47, no. 6, pp.53-57, June 2004.

[3] Yong Wang, Garhan Attebury and Byrav Ramamurthy, "A survey of security issues in wireless sensor networks", *IEEE Communications Survey and Tutorials*, vol. 8, no.2, pp.2-23, Second Quarter 2006.

[4] Kalpana Sharma, M.K.Ghose and Kuldeep, "Complete security framework for wireless sensor network", *International Journal of Computer Science and Information Security*, vol.3, no.1, pp.196-202, July 2009.

[5] Pirzada and C.McDonald, "Establishing trust in pure adhoc networks", *Proceedings of the 27th Australasian Computer Science Conference*, Dunedin, New Zealand, vol.26, no.1, pp.47-54, January 2004.

[6] Mohammad Momani and Subhash Challa "Survey of trust models in different network domains" *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, vol. 1, no. 3, pp. 1-19, September 2010.

[7] Charles E. Perkins, "Ad hoc On-demand Distance Vector Routing", *RFC 3561, IETF MANET Working Group*, July 2003.

[8] Asar Ali and Zeeshan Akbar, "Evaluation of AODV and DSR routing protocols of wireless sensor networks for monitoring applications", *Thesis Report, Department of Electrical Engineering with Telecommunication*, Blekinge Institute of Technology, Sweden, October 2009.

[9] Georgy Sklyarenko, "AODV routing protocol", *Seminar Technische Informatik*, Institut fur Informatik, Freie Universitat, Berlin, Germany, July 2006

[10] Sachin Sharma, H.M.Gupta and S.Dharmaraja, "EAGR: Energy aware greedy routing scheme for wireless Adhoc networks", *International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, David Hume Building and William Robertson Building, Edinburgh, UK, pp.122-128, June 2008.

[11] Uk-Pyo Han, Sang-Eon Park and Young-Jun Chung, " An efficient energy aware routng protocol for wireless sensor networks", *Proceedings of International Conference on Wireless Networks*, Las Vegas, pp.122-127, June 2006.

[12] Asad Amir Pirzada , Amitava Datta and Chris McDonald, "Trust-based routing for adhoc wireless networks", *Proceedings of 12th IEEE International Conference on Networks* , vol.1, pp.326-330, November 2004.

[13] Kamal Deep Meka, Mohit Virendra and Shambhu Upadhyaya, "Trust based routing decisions in mobile adhoc networks", *Proceedings of 2nd Workshop on Secure Knowledge Management*, Brooklyn, New York, September 2006.

[14] H.C. Leligou, P.Trakadas, S.Maniatis, P.Karkazis and T.Zahariadis, "Combining trust with location information for routing in wireless sensor networks", *Research Article, Wireless Communications and Mobile Computing*, John Wiley and Sons Ltd., December 2010.

[15] I.Downard, "Simulating sensor networks in ns-2," NRL *Formal Report 5522-04-10*, Naval Research Laboratory, Washington, May 2004.

8. AUTHORS PROFILE

P. Samundiswary received the B.Tech degree (1997), M.Tech degree (2003) and Ph.D. (2011) in the department of Electronics and Communication Engineering from Pondicherry Engineering College affiliated to Pondicherry University, India. She is having 13 years of teaching experience. She is currently working as Assistant Professor in the Dept. of Electronics Engineering, School of Engineering and Technology, Pondicherry University, Pondicherry, India. Her research interests include Wireless Communication and Wireless Networks.