Enhanced Ad-hoc On-Demand Distance Vector Routing Algorithm

Nidhi Beniwal*
Department of computer science and engineering
GGSIPU,Dwarka, New Delhi, India
nidhibeniwal1991@gmail.com
orcid id: 0000-0002-5791-5899

Mamta Mittal
Department of computer science and engineering
Govind Ballabh Pant Engineering College, New Delhi, India
mittal.mamta@gov.in
orcid id: 0000-0003-0490-4413

Lalit Mohan Goyal
Department of computer science and engineering
Bharti Vidyapeeth college of engineering, New Delhi, India
lalitgoyal78@rediffmail.com
orcid id:0000-0003-4618-0281

Monika
Research Scholar, Department of computer science & engineering,
University school of information & communication technology, GGSIPU, New Delhi, India
monika.mehta30@yahoo.com
orcid id: 0000-0001-5070-2818

Abstract - Several paths between a source and destination node in a network is established by Multipath routing. To achieve efficient, secure and reliable routing using multiple alternative paths for ad-hoc networks, we have proposed EAODV. The energy consumption and security are problems in the wireless networks. As mobile units are dependent on battery power, the energy consumption need to be minimized. One of the key issues is security in such networks, mainly for those security applications, like military strategic operations. In EAODV, energy conservation and security have been considered with multiple path routing. Count helps in detecting an attacker node and we need not follow the path containing attacker node out of multiple possible paths. Energy is saved by not doing route discovery again and again. RSA encryption in the route reply provides security. In route reply packet, we add additional field for RSA algorithm. When a destination node forwards RREP packet, each node, through which the RREP is unicasted, performs the decryption to check the authenticity of the packet. Thus, using EAODV, secured and energy optimized routing based on multiple paths in a WSN can be possible.

Keywords: encryption; multipath; routing; sensor network.

1. Introduction

Wireless Sensor network is a technology that will play a prime part in sensing, assembling and disseminating information about the environmental phenomena [Stajano (1999)][Ahmed(2005)]. There are large number of small sensor nodes which are of tiny size, and are placed densely in the environment. Reliability can be achieved in ad-hoc networks through multiple path routing. Several paths between a source and destination node in a network is established by Multipath routing. The routing must be secured and energy saving. Routing in such networks is, generally, multi-hop since units may not be within the wireless transmission range of one another. Also, as units can move freely and randomly, routes can often get disconnected. Thus, routing protocols for such networks should be distributed and must adapt to frequent changing on the network topology, while keeping the communication overhead to a minimum. The energy consumption and security are major challenges in the wireless networks [Virmani (2013a)] [Montoya (2013)]. It is important to minimize the consumption of energy, as the mobile units are dependent on battery power. One of the key issues is security in ad hoc networks, mainly for those security applications, like military strategic operations [Virmani (2013b)].

The paper contains seven sections. Section 1 is Introduction, section 2 is literature survey, section 3 is existing work, section 4 is work proposed, section 5 contains results and analysis, section 6 contains advantages of proposed work, and section 7 is conclusion and future scope.

2. Literature Survey

Our work bears resemblance to other research efforts in the literature. This particular section gives an overview of such techniques:

In [Li (2010)], author analyzed major security issue and presented implementation of the most cost efficient and appropriate method of procuring the network. Wireless sensor networks are characterized by extremely constrained computational and energy resources, and an ad hoc workable environment. Security becomes extremely important, when such networks are placed in a hostile environment, as they are vulnerable to many types of destructive attacks.

In [Burgner (2011)], author reviewed WSN's security. The areas covered are: routing protocols and architecture; issues related to security that include context and design, and also confidentiality, integrity, and authenticity; algorithms; and performance issues for WSN design. Performance of the Self-Originating Wireless Sensor Network (SOWSN), Algorithm for Data Security (PADS), and methods for in-network processing were investigated in further detail with SOWSN showing the best performance.

In [Roy (2014)], the researchers had given a loss-pliant framework for aggregation which is known as synopsis diffusion, and duplicate insensitive algorithms are used on top of multiple path routing strategy to compute aggregates, accurately. Still, this framework for aggregation does not look into the difficulty of sub aggregate false values bestowed by nodes which are compromised. The attack may lead to huge errors in the computed aggregate at the base station, that is the root node of the hierarchy of aggregation. The author has made the approach for synopsis diffusion, secured against the above attack propelled by compromised nodes. Basically, even in the presence of such attack, to compute securely the predicate count or sum, an algorithm is presented. The computation algorithm is attack-resilient and it evaluates the aggregate by straining out the role played by the compromised nodes in the aggregation hierarchy.

In [Nasser (2007)], author proposes a protocol for routing known as SEEM: Secure and Energy-Efficient multipath Routing protocol. Multiple paths are used in SEEM alternately as the path between two nodes for communication and thus extends the network lifetime. Also, SEEM is defiant to some particular attacks which has the nature of pulling the traffic across the harmful nodes through a route announced towards the destination. There are three phases in SEEM: Construction of Topology, Transmission of Data and Maintenance of Route. First phase is configuring the network topology; second phase i.e. Transmission of data is the working phase; and in third phase, the available energy is updated on each node by the base station and a new path is re-selected towards the source node.

In [Ehsan (2012)], routing techniques for WMSNs, that should be energy-efficient, are investigated together with the issues of performance of every strategy. The researchers define the challenges in routing protocols' design for WMSNs with the constraints in prevailing methods.

3. Existing Work: AODV

The Ad-hoc On-Demand Distance Vector (AODV) algorithm allows active, self-starting, multi-step routing among mobile nodes taking part, that is needed initiating and maintaining an ad hoc network[Perkins (2003)]. Through AODV, the nodes acquire paths to new destinations. AODV does not need nodes to preserve paths to destinations which are not in active communication. This algorithm uses sequence number of destination for each route entry, which is one of its recognizing feature. The destination creates its sequence number which is to be incorporated with any route information it conveys to requesting nodes. Loop freedom is safeguarded using destination sequence numbers. A requesting node is needed to select the one of given two routes, with the greatest sequence number. Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies.

In this, when a node Sender(S) needs to send a message to node Destination(D). A RREQ message is initiated by S, if there is no path. The RREQ message contains the IP addresses of Sender and Destination; the CSN(current sequence number) of Sender and LNSN(the last known sequence number) of Destination; a BID(broadcast ID) from Sender. This BID is increased by 1 each time S forwards a RREQ message. Assume that a node P gets the RREQ from S. It is checked whether P has received this RREQ earlier. Every node saves the <BID, IP-address> pairs for all the recently received RREQs. If P has already received this RREQ from S,RREQ is discarded by P. Else, the request is processed by P, as P sets up a reverse route entry for the S in its route table. The entry will contain the IP address and CSN of S, number of hops to S and the neighbor's address from where P got the RREQ. RREP is reply packet.

4. Proposed work- EAODV

In the proposed work, AODV has been used and various modifications are proposed in that.When destination node is not X, the packet are broad-casted to its neighbor. X then sets up a reverse route entry for the S in its route table. This will contain the IP address and CSN of S, number of hops to S and the neighbor's address from where X got the RREQ. Another fields are added which are the node id of neighbor, to which X sends RREQ, sending time of X, receiving RREQ time of neighbor of X and count.Count is the difference of sending and receiving time. This count helps detecting an attacker node and we need not follow that path. Multiple paths have been used by keeping count of no. of hops so that we need not do route discovery, thus saving energy.

Due to congestion in the network, sometimes, expiration of timer may be there and the system may report a false positive node that is false attacker node detection. To overcome this, the concept of encryption is used and also uses RSA algorithm. This encryption provides security from attacker nodes. In route reply packet, we add additional field for RSA algorithm. When a destination node forwards RREP packet, each node through which the RREP is uni-casted performs the decryption to check the authenticity of the packet.

Using modified AODV i.e EAODV with multipath routing by introducing no. of hops and RSA encryption, we propose secure and energy optimized routing algorithm based on multiple path in wireless sensor networks [Sudhashini (2013)] [Akyildiz (2002)].

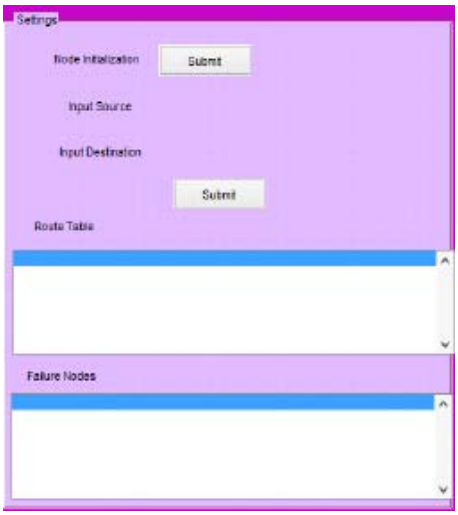
5. Results And Analysis

In this particular section, the results and analysis of proposed work has been shown through snapshots, by performing the proposal using MATLAB.

I. Sensor Nodes Area

This is the area where all sensor nodes will be shown after their initialization. Their routes will also be shown after providing input source and destination. The Routing table, failure nodes area, and table entry area are also separately shown in figure 1.

(a)



(b)

(c)

Fig. 1: Sensor nodes area. (a)Nodes Area (b) Routing Table (c)Table entry

II. *N*ode Initialization

On clicking the submit button for node initialization, all nodes with their respective IP addresses will be shown in the sensor node area. All nodes are named to be distinguished from others. These nodes are shown in figure 2.

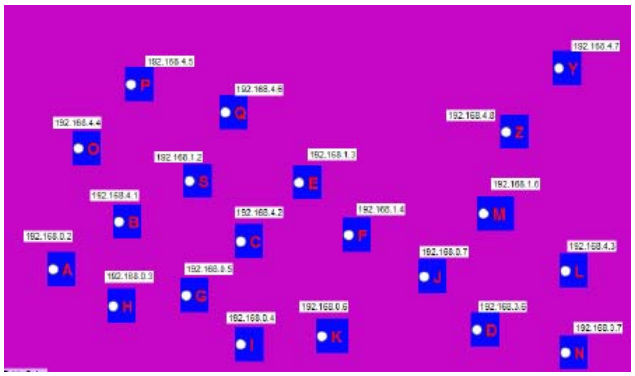


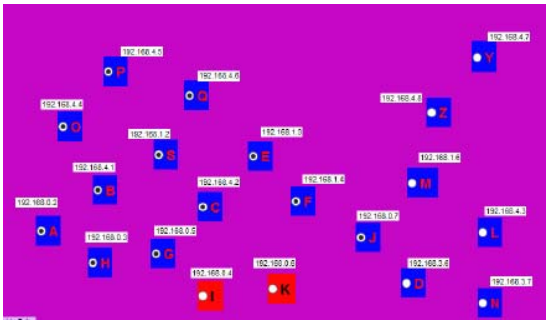
Fig. 2: Node Initialization: Nodes with their ip addresses

III. *R*outes between Source and Destination

The source and destination nodes need are to be entered by user in the respective fields. On the basis of these two, the possible routes will be discovered.

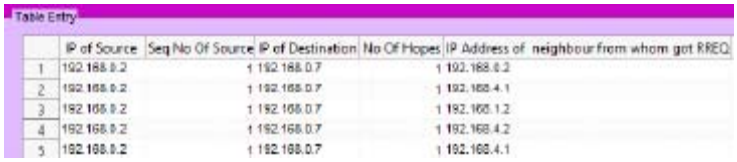
1. All Possible Routes

On submitting the source and destination nodes, the RREQ packet will be broadcasted by the source node through all possible routes via intermediate nodes to the final destination node. While broadcasting is in process, the table entry with various parameters are filled in the table and also various parameters are calculated, as shown in fig3. A parameter count is calculated using receiving and sending times. Using count failure nodes can be detected. In the route table, all possible routes are shown; even the routes with failure nodes.



(a)

(b)



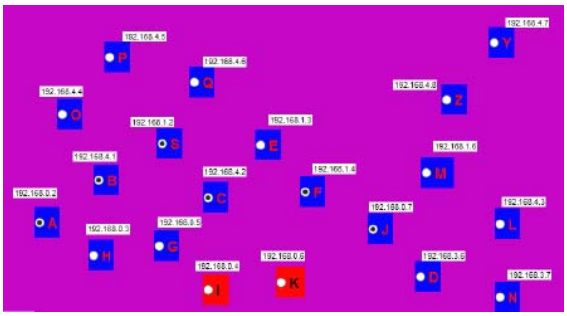
(c)

(d)

Fig. 3: Possible Routes (a) Nodes Area (b) Routing Table (c), (d) Table Entry

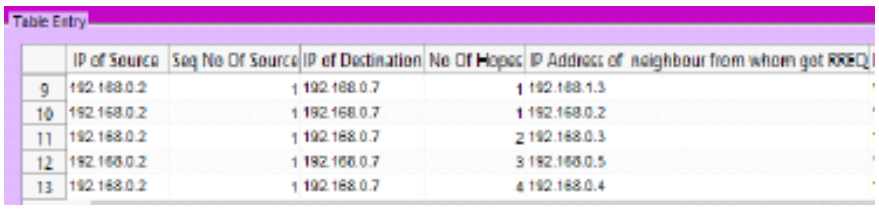
2. Routes rejecting failure nodes route

After detection of failure nodes, the route containing these nodes will be rejected. And the routes other than rejected will be retained, as shown in figure4. Out of these, the shortest route will be used to reply by destination to the source. The destination will send RREP packet. The RREP packet also includes encryption which will provide security even if failure node was not detected initially and the faulty path was chosen.



(a)

(b)



IP Address of which forward the RREQ	Recieving Time	Sending Time	Count	Detection	Node I
192.168.0.7	7	8	0		F
192.168.0.5	2	3	0		H
192.168.0.4	3	4	0		G
192.168.0.6	4	14	1	Failure Node	I
192.168.0.7	15	27	1	Failure Node	K

(c)

Fig. 4: Routes rejecting failure node route. (a)Nodes Area (b) Routing Table (c)Table Entry

IV. *R*SA Algorithm for each Node

RSA Algorithm has been applied on each node to make the network secure. The code for RSA algorithm at a particular node is as shown in figure 5.

```
d=515
Public key is (1283,1739)
Private key is (515,1739)ASCII equivalent of message
    74


The encrypted message is
    1130
The decrypted mes in ASCII is
    74
The decrypted message is: J
```

(a)

```
d=1183
Public key is (7,1739)
Private key is (1183,1739)ASCII equivalent of message
    65


The encrypted message is
    1339
The decrypted mes in ASCII is
    65
The decrypted message is: A
```

(b)

Fig. 5: Depicting RSA at nodes. (a) RSA at Node J, (b) RSA at Node A.

6. Advantages

The proposed model has following advantages over the existing AODV algorithm:

- We have a kind of double verification, one is through our RREQ packet and other is through RSA encryption algorithm.
- Removal of false nodes in the network.

7. Conclusion and Future Scope

Sensor network is a technology which will play an important part in sensing, assembling and disseminating information about environmental phenomena. It consists of large number of small sensor nodes which are of tiny size and are densely placed in the environment. The main aim of sensor network is to detect and report events occurring within the range of sensor network. Multiple paths between a source and destination node in a network is established by Multipath routing. Reliability is achieved in ad-hoc networks through multipath routing. The energy consumption and security are challenges in the wireless networks. As mobile units are dependent on battery power, it is important to minimize the energy consumption. Security is a key issue in ad hoc networks, especially for those security applications, like military strategic operations.

In this paper, EAODV has been proposed which is a secure and energy optimized routing algorithm based on multiple paths in wireless sensor networks and AODV(ad hoc on demand distance vector routing). This proposal helps saving energy by not doing route discovery and make the sensor network secure using RSA algorithm. Multiple paths have been used here. Implementation for initialization of sensor nodes and route paths between source node and destination node; their route entry tables; indicating failure nodes; and implementation of RSA in route reply packet have been done. Thus, using this secured and energy optimized routing based on multiple paths in a WSN can be possible.

As a future work, more work need to be done on other parameters also with energy and security. Lifetime of WSN also need to be maximized based on various parameters like distance between nodes, energy, cost etc.

8. References

[1] Ahmed, N., Kanhere, S. S., & Jha, S. (2005). The holes problem in wireless sensor networks: a survey. ACM SIGMOBILE Mobile Computing and Communications Review, 9(2), 4-18.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications magazine, 40(8), 102-114.

[3] Burgner, D. E., & Wahsheh, L. A. (2011, April). Security of wireless sensor networks. In Information Technology: New Generations (ITNG), 2011 Eighth International Conference on (pp. 315-320). IEEE.

[4] Ehsan, S., & Hamdaoui, B. (2012). A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Communications Surveys & Tutorials, 14(2), 265-278.

[5] Li, Y. X., Qin, L., & Liang, Q. (2010, December). Research on wireless sensor network security. In Computational Intelligence and Security (CIS), 2010 International Conference on (pp. 493-496). IEEE.

[6] Montoya, G. A., Velásquez-Villada, C., & Donoso, Y. (2013). Energy optimization in mobile wireless sensor networks with mobile targets achieving efficient coverage for critical applications. International Journal of Computers Communications & Control, 8(2), 247-254.

[7] Nasser, N., & Chen, Y. (2007). SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks. Computer Communications, 30(11), 2401-2412.

[8] Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[9] Roy, S., Conti, M., Setia, S., & Jajodia, S. (2014). Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact. IEEE Transactions on Information Forensics and Security, 9(4), 681-694.

[10] Stajano, F. (1999, April). The resurrecting duckling. In International workshop on security protocols (pp. 183-194). Springer Berlin Heidelberg.

[11] Sudhashini, P., Prema, G., & Fairosebanu, A. (2013) Multi-Path Routing and Secure Data Collection In Wireless Sensor Networks International Journal Of Engineering And Computer Science ISSN:2319 – 7242 Volume 2 Issue 7 , Page No. 2291-2295

[12] Tilak, S., Abu-Ghazaleh, N. B., & Heinzelman, W. (2002). A taxonomy of wireless micro-sensor network models. ACM SIGMOBILE Mobile Computing and Communications Review, 6(2), 28-36.

[13] Virmani, D., Mandal, G., Beniwal, N., & Talwar, S. (2013a). Dynamic Data Aggregation Tree for Data Gathering in Wireless Sensor Network. proceedings of International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2(3), 226-230.

[14] Virmani, D., Beniwal, N., Mandal, G., & Talwar, S. (2013b). Enhanced Tiny Encryption Algorithm with Embedding (ETEA). arXiv preprint arXiv:1306.6920.