ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/101219, December 2016* ISSN (Online) : 0974-5645

Secure and Efficient Information Propagation using Pushback Algorithm based Routing for Wireless Networks

Rupinder Singh and Dinesh Kumar

Department of Computer Science, Guru Kashi University, Sardulgarh Road, Talwandi Sabo, Bathinda - 151302, Punjab, India; dca.rupinder@gmail.com, kdinesh.gku@gmail.com

Abstract

Objectives: The proposed model is based upon the efficient and secure routing with the amalgamation of the authentication protocol for the realization of the secure routing protocol. **Methods/Statistical Analysis:** The proposed model is based upon the efficient and secure routing with the amalgamation of the authentication protocol for the realization of the secure routing protocol. The proposed model is aimed at protecting the routing mechanism from the false route injections. The proposed model utilizes the lightweight authentication scheme for the purpose of security enforcement over the wireless network. **Findings:** The experimental results have been collected in the form of various network and routing performance parameters, where the proposed model has been found efficient and stable in comparison with the existing model. **Application/Improvements:** The proposed model has been primary improved for the routing efficiency along with the security perspectives in order to protect the wireless networks from the network attacks.

Keywords: Efficient Routing, Pushback Mechanism, Secure Routing, Stable Wireless Routing, Lightweight Authentication

1. Introduction

Over the second half a century, computers have exponentially raised in process power and at a similar time cut in each size and worth[1]. These fast advancements crystal rectifier to a awfully quick market within which computers would participate in the lot of and more of our society's daily activities[2]. In recent years, one such revolution has been going down, wherever computers are getting therefore little so low-cost, that single-purpose computers with embedded wireless devices are considered virtually sensible from each economical and theoretical points of read[3]. Wireless networks are considered as the points with starting to become a reality, and so a number of the long unnoted limitations became a vital space of analysis[4].

Figure 1 shows that the latest analysis on wireless networks, wherein focus has made to overcome limitations of the wireless networks such as: restricted energy resources, varied energy consumption supported location, high price of transmission, and restricted process capabilities[4-5]. All of those characteristics of wireless networks are complete opposites of their wired network counterparts, within which energy consumption isn't a problem, transmission price is comparatively low-cost, and therefore the network nodes have lots of process capabilities[6]. Routing approaches that have worked therefore well in ancient networks for over twenty years won't do for this new generation of networks[7].

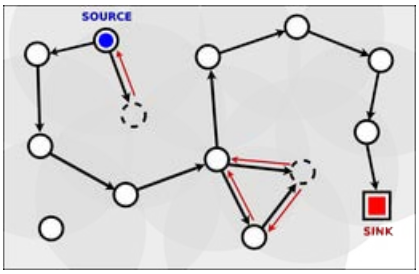

Figure 1. Basic architecture of the linear wireless network with the single path scenario with route selected towards the sink node.

* *Author for correspondence*

Besides increasing the period of time of the device nodes, it's preferred to distribute the energy dissipated throughout the wireless network so as to reduce maintenance and maximize overall system performance. Any communication protocol that involves synchronization between peer nodes incurs some overhead of putting in the communication[8]. Wireless routing or agglomeration protocols confirm whether or not the advantages of additional advanced routing algorithms overshadow the additional management messages every node must communicate Figure 2[9].

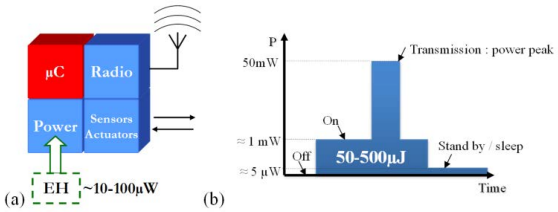

Figure 2. a) The architecture of the wireless node and (b) Overall energy consumption tracking over the wireless node.

Every node might build the foremost abreast of call relating to its communication choices if they'd complete data of the complete topology and power levels of all the nodes within the network[10]. This so proves to yield the most effective performance if the synchronization messages aren't taken under consideration. However, since all the nodes would invariably have to be compelled to have world data, the value of the synchronization messages would ultimately be terribly pricey[11]. For each the diffusion and agglomeration algorithms, we'll analyze each realistic and optimum scheme so as to achieve additional insight within the properties of each approaches Figure 3[12-13].

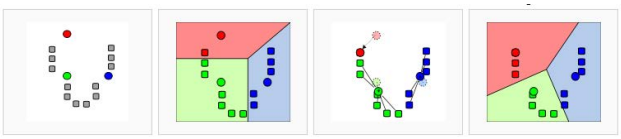

Figure 3. A standard clustering algorithm example.

Geo-routing includes the location of various nodes in the form of location coordinates in order to determine the direction of the traffic flow. By using geographic or geo-location aware routing, length of the routes can be significantly decreased and the packet delivery ratio can be improved with better data propagation perspectives of geo-location aware routing scheme. This rule provides the guarantee of the delivery of packets from supply node to destination node. The steered rule is predicated on the hybrid cluster theme. The hybrid cluster theme divides the network into cliques in keeping with the present energy economical protocol. Every pack encompasses a cluster head that is split into teams in keeping with the energy economical hierarchic cluster. Energy economical routing protocol for heterogeneous wireless detector network is projected by aforesaid mountain. The network localization plays the vital role in the wireless routing[14]. This protocol conjointly selects a cluster head that have a highest energy to gather the data regarding all member of that cluster. The cluster head sends the packets to the gateways. The prominent rule for connecting nodes has been enforced in the various models implemented to tackle the problems related to the routing and its security[15]. The hierarchic cluster based mostly energy economical routing protocol[16]. In keeping with the wireless routing protocols with privacy enabled, the bottom station chooses the cluster heads (CH) with the certain rules[17]. This choice is predicated to 2 stages. In initial stage all participates nodes are entitled and listed into cluster heads list. This list is predicated on the space of every node from its base station[18]. Multiple times anode is mentioned into cluster head list[19]. The cluster head generates 2 states for the member of the cluster list. Initial is that the Sleep and second is that the TDMA based mostly transmit[20]. The wireless detector network could be a combination of detector nodes for grouping varied knowledge like temperature, sound, location etc. Wireless detector networks are applied on several fields like observance, healthcare, military field etc. Exchange the detector nodes could be a terribly troublesome task for those nodes that have restricted battery backup. Energy potency could be a major think about wireless detector network. The choice of energy economical cluster head in keeping with K-means rule is projected[21]. This rule is predicated on minimum distance between head and therefore the cluster members. The geocasting method related to the hop-to-hop node based network[22]. This rule provides comparison of the performance of all hop-to-hop neighbor nodes. Every node keeps the data regarding its neighbors[23]. ALBA-R is the protocol for convergence and geocasting in wireless detector networks. ALBA-R has the inter-layer integration with geographic routing based multicast acknowledgement rivalry for choice on relay and cargo equalization based protocol, in addition as a mechanism to find and avoid property holes (arc). ALBA and Rainbow (ALBA-R) to resolve the routing drawback along around a dead finish while not intensive

air graphics techniques comparable to leveling and routing face[24]. Through simulations based mostly NS2, we have a tendency to show that the ALBA-R considerably outperforms different protocols and convergence and over casting solutions to deal with property holes, particularly in terms of important data in the wireless networks with the less number of the nodes. The new routing algorithm has been designed to work around the connectivity holes by utilizing the geographically aware wireless nodes in the networks[25]. To cut back latency from finish to finish and grow to high traffic, ALBA-R is predicated on a cross-promoting layer relay nodes choice mechanism which might transmit traffic a lot of with efficiency and dependably, in keeping with traffic and therefore the quality of the link.

2. Experimental Design

The proposed model has been designed for the minimization of the energy consumption over the wireless networks with the smart and higher energy level based path selection for the efficient and secure transmission of the network data. The proposed model has been equipped with the network load aware routing path selection algorithm with the utilization of the pushback algorithm along with the lightweight authentication as the integrated module in the pushback agent for the robustness of the proposed model's security and data propagation level.

Routing Discovery: The pushback mechanism has been utilized in the proposed model which proposes the dual layered protocol for the realization of the efficient and secure wireless routing protocol. The proposed pushback model has been enhanced for the dual layer authentication model, which utilizes the network performance evaluation in the form of the node availability in the network connectivity, available queue length over the target wireless nodes and security level of the target nodes in order to protect the nodes from the external attacks. The pushback mechanism in the proposed secure routing model has been designed and designated to work as the agents and programmed to response in the connectivity layers in order protect against the attacks along with the multi factor wireless node's analytical study. The following algorithm defines the proposed pushback agent model in detail:

Algorithm 1: Secure and efficient pushback routing algorithm (SEPRA)

- *Initiate the wireless cluster*
- *Connect the wireless nodes under the localization process during the startup phase.*
- *Nodes starts sending the neighbor setup phase*
- *The nodes builds their neighbor table under the neighbor formation process using the pre-shared security model*
- *When a wireless node needs to propagate the data, routing algorithm starts the route discovery process*
- *Routing algorithm calls the pushback module*
- *Pushback module request the connection over the other node*

a. Other node replies with the initial acknowledgement
b. If initial acknowledgement is found successful
i. Query the node availability
ii. Query the available queue size
iii. Return the status
a. If b(iii) returns true, initiate the authentication process
i. Ask for the pre-shared information
ii. If pre-shared information matches
iii. Send the standard query code
iv. The sensor node on other end replies with the standard reply code generated from the standard query code
v. If query code is found true
1. Establish the communication
vi. Otherwise
1. Return the request denial

- *If 7(c)(v) returns true*

a. Start the routing discovery process

3. Result Analysis

This section includes the observations and testing results of the proposed model in order to evaluate its performance in the variety of the perspectives in the wireless networks. The variety of the performance measures has been utilized for the observation of the performance improvement in the proposed authentication and energy efficiency based routing algorithm.

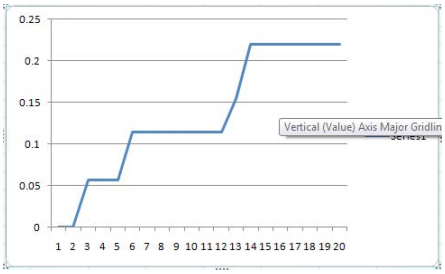

Figure 4. Performance evaluation based upon the transmission delay.

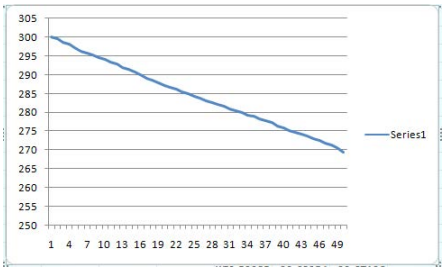

Figure 5. Performance evaluation based upon the energy consumption.

The Figure 4 describes the performance of the proposed routing model on the basis of the network reaction time in the form of the end-to-end transmission delay, which indicates the total time taken for the data propagation from the sourcing point to the destination. The CBR (constant bit rate) model has been utilized to transmit the data among the simulation topology, which propagates the data on the rate of 100 Kbps over pre-allocated wireless channel among the given topology. The efficient authentication delay of nearly 0.23 milli-seconds has been observed under the performance assessment survey. The proposed model has been designed for the energy efficient network node's current performance parameter discovery and the robust security model based upon the pre-shared information based authentication model. The energy efficiency plays the vital role in elongation of the wireless networks in order to collect the maximum information from the target source, where the wireless network has been deployed. The deep scanning activities has been imposed over the data in the ingress and egress queues in order to detect the anomalies in the wireless networks. The proposed model is also based upon the pre-shared information based network parameter evaluation for the implementation of the security model over the given transmission link. The proposed model relies upon the injection of the security information over the network nodes before deploying them in the real-time network. This pre-shared information is utilized for the multifactor authentication, which utilizes the pre-embedded method, which computes reply key on the target nodes in response to the query information propagated from the wireless node to the target node. The proposed wireless network model shows that it consumes less than 1 millijoule or energy to transmit one standard topology packet, which is clearly shown from the Figure 5. This performance shows the robustness of the proposed model.

4. Conclusion

The proposed scheme has been specifically designed to protect the wireless networks against the wireless false route injection attacks, which may cause the wormhole attacks in the wireless networks. The proposed routing algorithm is equipped with the robust authentication mechanism to ensure the node integrity during the wireless networks in action. The energy efficiency can be compromised with the amalgamation of the lightweight but robust authentication model over the routing algorithm to protect the wireless network routing algorithm. The proposed model has been analyzed under the variety of the performance measures, where the proposed model has been analyzed for the variety of the issues related to the security and performance. The network topology with the standard paradigms has been utilized for the assessment of the performance of the proposed model. The performance measures of the overall energy consumption along with the end-to-end transmission delay have been utilized for the proposed model's performance evaluation. The strong improvement has been observed in the case of the proposed model in comparison with the existing models.

5. References

1. Alessandro C, Nati M, Petrioli C, Rossi M, Zorzi M. IRIS: Integrated data gathering and interest dissemination system for wireless sensor networks. Ad Hoc Networks. 2013; 11(2):654-71.
2. Ananth R, Ratnasamy S, Papadimitriou C, Shenker S, Stoica I. Geographic routing without location information. ACM, Proceedings of the 9th annual international conference on Mobile computing and networking. 2003; p. 96-108.
3. Bomgni AB, Frederic MJ. An energy-efficient clique-based geocast algorithm for dense sensor networks. Communications and Network. 2010.
4. Palden BS, Rai P, Kumar H, Sarma D. Energy efficient cluster based routing protocol for Wireless Sensor Networks. IEEE, 2012 International Conference on, Computer and Communication Engineering (ICCCE). 2012; p. 603-7.
5. Ben AS, Ezzati A, Hssane AB, Hasnaoui ML. Hierarchical adaptive balanced energy efficient routing protocol (HAB-RP) for heterogeneous wireless sensor networks. IEEE, 2011 International Conference on Multimedia Computing and Systems (ICMCS). 2011; p. 1-6.
6. Frey H, Hrup RS, Stojmenovic I. Springer-Verlag: Routing in Wireless Sensor Networks, Guide to Wireless Sensor Networks. Misra, Woungang I and Misra SC, eds. ch. 4. 2009 May; p. 81-112.

7. Vinoth K, Bhavani S. An Efficient Secured Localization based Optimized Energy Routing for MANET. Indian Journal of Science and Technology. 2015 Dec; 8(35):1-7.
8. Aakash D, Shanthi P. Lightweight Security Algorithm For Wireless Node Connected with IoT. Indian Journal of Science and Technology. 2016 Aug; 9(30):1-8.
9. Takagi H, Kleinrock L. Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals. IEEE Trans. Comm. 1984 Mar; 32(3):246-57.
10. Stojmenovic I. Position Based Routing in Ad Hoc Networks. IEEE Comm. Magazine. 2002 Jul; 40(7):128-34.
11. Moaveninejad K, Song W, Li X. Robust Position-Based Routing for Wireless Ad Hoc Networks. Elsevier Ad Hoc Networks. 2005 Sept; 3(5):546-59.
12. Kumar S, Helmy A, Govindan R. On the Effect of Localization Errors on Geographic Face Routing in Sensor Networks. Proc. IEEE/ACM Third Int'l Symp. Information Processin in Sensor Networks (IPSN '04). 2004 Apr; p. 71-80.
13. Barriere L, Fraigniaud P, Narayanan L, Opatrny J. Robust Position-Based Routing in Wireless Ad Hoc Networks with Unstable Transmission Ranges. J. Wireless Comm. and Mobile Computing. 2001; 2(3):141-53.
14. Battelli M, Basagni S. Localization for Wireless Sensor Networks: Protocols and Perspectives. Proc. IEEE Canadian Conf. Electrical and Computer Eng. (CCECE '07). 2007 Apr; p. 1074-77.
15. Zorzi M. A New Contention-Based MAC Protocol for Geographic Forwarding in Ad Hoc and Sensor Networks. Proc. IEEE Int'l Conf. Comm. (ICC '04). 2004 Jun; 6:3481-85.
16. Casari P, Nati M, Petrioli C, Zorzi M. Efficient Non-Planar Routing around Dead Ends in Sparse Topologies Using Random Forwarding. Proc. IEEE Int'l Conf. Comm. (ICC '07). 2007 Jun; p. 3122-29.
17. Park GY. A Novel Cluster Head Selection Method based on K-Means Algorithm for Energy Efficient Wireless Sensor Network. Advanced Information. 2013.
18. Petrioli C. ALBA-R: Load-balancing geographic routing around connectivity holes in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2014; 2(5):529-39.
19. Fang Q, Gao J, Guibas LJ. Locating and Bypassing Holes in Sensor Networks. ACM Mobile Networks and Applications. 2006 Apr; 11(2):187-200.
20. Huang Q, Bhattacharya S, Lu C, Roman GC. FAR: Face-Aware Routing for Mobicast in Large-Scale Networks. ACM Trans. Sensor Networks. 2005 Nov; 1(2):240-71.
21. Fonseca R, Ratnasamy S, Zhao J, Culler D, Shenker S, Stoica I. Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets. Proc. Second Conf. Symp. Networked Systems Design and Implementation (NSDI '05). 2005 May; 2:329-42.
22. Ravi S, Ashish KL, Amit S. To Enhance the Security in Wireless Nodes using Centralized and Synchronized IDS Technique. Indian Journal of Science and Technology. 2016 Aug; 9(32):1-5.
23. Basagni S, Nati M, Petrioli C. Localization Error-Resilient Geographic Routing for Wireless Sensor Networks. Proc. IEEE GLOBECOM. 2008 Nov/Dec; p. 1-6.
24. Shim YC, Ramamoorthy CV. Monitoring and control of distributed systems. Systems Integration'90, IEEE, Proceedings of the First International Conference on Systems Integration. 1990.
25. Xu JQ. Study on WSN topology division and lifetime. IEEE, 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE). 2011; 1.