SECURE AND EFFICIENT INFORMATION PROPAGATION USING PUSHBACK ALGORITHM BASED ROUTING FOR WIRELESS NETWORKS

Rupinder Singh, Dr. Dinesh Kumar
Department of Computer Science, Guru Kashi University, Sardulgarh Road, Talwandi Sabo, Bathinda- 151302, Punjab, India;

ABSTRACT— The wireless networks are the networks connected over the wireless spectrum allocated to the particular wireless technologies. The wireless networks have grown their popularity as the wireless local area networks (WLAN) or Wi-Fi, Wi-Max, Bluetooth, Zigbee, etc. The wireless networks have been utilized under the variety of the real-time applications such as wireless LAN, wireless personal area networks (WPAN), wireless long range communications (WLRC), etc. The routing protocols plays the significant role in the inter connectivity of the wireless nodes by discovering the routes in the given network. There are two primary routing paradigms for the wireless networks, reactive and proactive routing, where the reactive routing is the trigger event based routing and finds the routes when required, whereas the proactive routing protocols rely upon the collection of the maximum useful routes irrespective of their current requirements. 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. 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.

INDEX TERMS: Wireless authentication, Energy efficiency, Lifetime elongation, Balanced energy routing.

I. 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. 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. 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. 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.

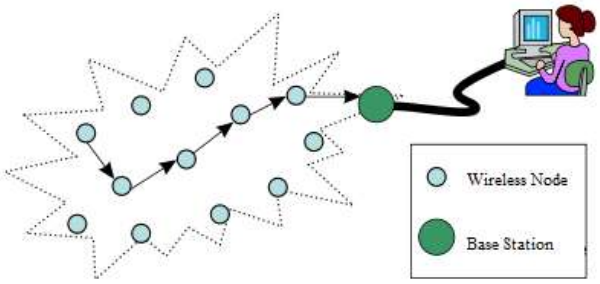

FIGURE 1.1: The basic architecture of the wireless network consisting of the centralized based network evaluation

In latest analysis on wireless networks, the researchers decide to determine and overcome limitations of the wireless networks such as: restricted energy resources, varied energy consumption supported location, high price of transmission, and restricted process capabilities. 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. Routing approaches that have worked therefore well in ancient networks for over twenty years won't do for this new generation of networks

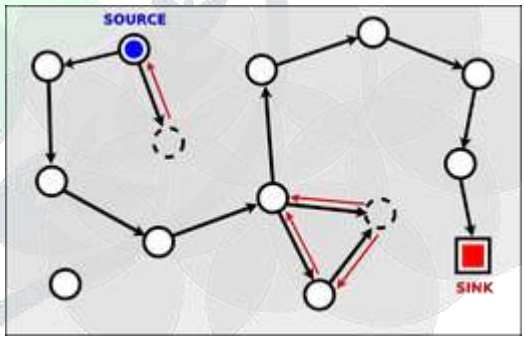

FIGURE 1.2: Basic architecture of the linear wireless network with the single path scenario with route selected towards the sink node

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. 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.

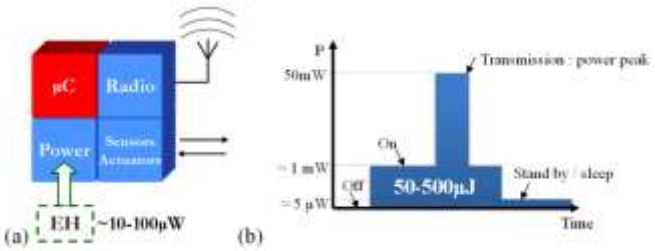

FIGURE 1.3: a) The architecture of the wireless node and (b) overall energy consumption tracking over the wireless node

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. 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. For each the diffusion and agglomeration algorithms, we'll analyze each realistic and optimum schemes so as to achieve additional insight within the properties of each approaches.

FIGURE 1.4: A standard clustering algorithm example

II. RELATED WORK

According to formulation geographical routing includes causation packets in this direction that is referred as a destination by providing most packet delivery quantitative relation [1]. 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 ALL et al. [2]. 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. XU Jiu-qiang et al. [6] projected the prominent rule for connecting nodes. Sonam Palden Barfunga et al. [3] projected a hierarchic cluster based mostly energy economical routing protocol. In keeping with this protocol the bottom station chooses the cluster heads (CH). 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. Multiple times anode is mentioned into cluster head list. 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. The wireless detector network could be a combination of detector nodes for grouping varied knowledge like temperature, sound, location etc. Wireless detector networks ar 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 by Geon et al. [4]. This rule is predicated on minimum distance between head and therefore the cluster members. Young-Chul wedge et al. [5] projected a geocasting method related to the hop-to-hop node based network. This rule provides comparison of the performance of all hop-to-hop neighbor nodes. Every node keeps the data regarding its neighbors. Through simulations based mostly NS2, we have a tendency to show that the AODV 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. Analysis of End to End Delay vs. time is done. End to end delay increases as the time is increased. Delivery of data is not safe when an attacker exists in the network; attacker drops all the data packets coming to it which tends minimum delivery of the packets. Thus, throughput decreases in the presence of attacker .The throughput in case of IDS scheme is approximate equal to the range of AODV which shows the better performance of routing in presence of IDS scheme over the attacker's effect.

III. III. 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. End to End delay is decreased considerably in the proposed model in any of the attacks and in any protocol is followed either it is AODV or DSR or any other. Throughput is increased also with the increase in the time.

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)

(1) Initiate the wireless cluster
(2) Connect the wireless nodes under the localization process during the startup phase.
(3) Nodes starts sending the neighbor setup phase
(4) The nodes builds their neighbor table under the neighbor formation process using the pre-shared security model
(5) When a wireless node needs to propagate the data, routing algorithm starts the route discovery process
(6) Routing algorithm calls the pushback module
(7) 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*
c. *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*
(8) *If 7(c)(v) returns true*
a. *Start the routing discovery process*

IV. 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.

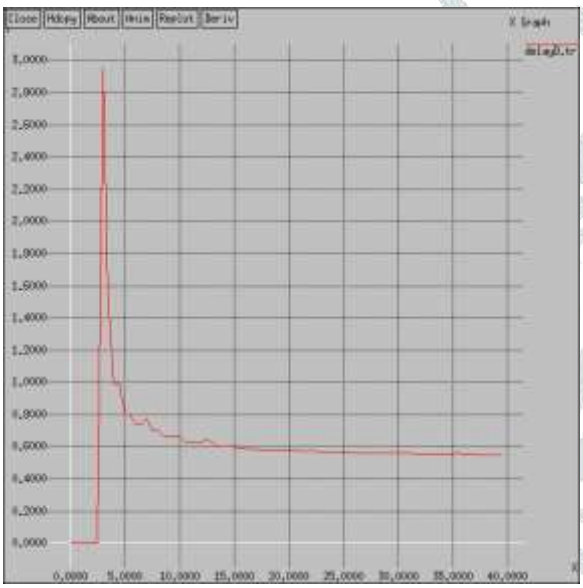

Figure 1: Performance evaluation based upon the transmission delay

The figure 1 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 efficient authentication delay of nearly 0.56 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 have 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.. This performance shows the robustness of the proposed model.

V. 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 communication between the wireless node and WLAN based platform service passes from many insecure network ingress or egress points, where there is higher risk of the communication data being exposed to the hackers. Hence, in this research we are going to propose a simple and secure key exchange mechanism to protect against the packet dropping attack in the wireless LANs. The AODV and DSR protocols would be particularly tested under the proposed model. The packet dropping attack would be tested with AODV and DSR routing protocols for WLANs in order to analyze their performance in the real-time sensor networks. The key exchange mechanism will utilize a unique key exchange mechanism with multiple random key combined together to prepare the query and reply keys. The strong improvement has been observed in the case of the proposed model in comparison with the existing models.

REFERENCES

[1] A. Camillo` , M. Nati, C. Petrioli, M. Rossi, and M. Zorzi, "IRIS: Integrated Data Gathering and Interest Dissemination System fo Wireless Sensor Networks," Ad Hoc Networks, Special Issue o Cross-Layer Design in Ad Hoc and Sensor Networks, vol. 11, no. 2, pp. 654-671, Mar. 2013.

[2] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica, "Geographic Routing without Location Information," Proc. ACM MobiCom, pp. 96-108, Sept. 2003.

[3] Alain Bertrand, Bomgni, and Myoupo Jean Frédéric. "An energy-efficient clique-based geocast algorithm for dense sensor networks." *Communications and Network* 2010 (2010).

[4] Barfunga, Sonam Palden, Prativa Rai, and Hiren Kumar Deva Sarma. "Energy efficient cluster based routing protocol for Wireless Sensor Networks." *Computer and Communication Engineering (ICCCE), 2012 International Conference on*. IEEE, 2012.

[5] Ben Alla, S., et al. "Hierarchical adaptive balanced energy efficient routing protocol (HABRP) for heterogeneous wireless sensor networks." *Multimedia Computing and*

Systems (ICMCS), 2011 International Conference on. IEEE, 2011.

[6] H. Frey, S. Ru¨ hrup, and I. Stojmenovic, "Routing in Wireless Sensor Networks," Guide to Wireless Sensor Networks, S. Misra, I. Woungang, and S. C. Misra, eds., ch. 4, pp. 81-112, Springer- Verlag, May 2009.

[7] H. Takagi and L. Kleinrock, "Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals," IEEE Trans. Comm., vol. 32, no. 3, pp. 246-257, Mar. 1984.

[8] I. Stojmenovic, "Position Based Routing in Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 7, pp. 128-134, July 2002.

[9] K. Moaveninejad, W. Song, and X. Li, "Robust Position-Based Routing for Wireless Ad Hoc Networks," Elsevier Ad Hoc Networks, vol. 3, no. 5, pp. 546-559, Sept. 2005.

[10] S. Kumar, A. Helmy, and R. Govindan, "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), pp. 71-80, Apr. 2004.

[11] L. Barrie`re, P. Fraigniaud, L. Narayanan, and J. Opatrny, "Robust Position-Based Routing in Wireless Ad Hoc Networks with Unstable Transmission Ranges," J. Wireless Comm. and Mobile Computing, vol. 2, no. 3, pp. 141-153, 2001.

[12] M. Battelli and S. Basagni, "Localization for Wireless Sensor Networks: Protocols and Perspectives," Proc. IEEE Canadian Conf. Electrical and Computer Eng., (CCECE '07), pp. 1074-1077, Apr. 2007.

[13] M. Zorzi, "A New Contention-Based MAC Protocol for Geographic Forwarding in Ad Hoc and Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC '04), vol. 6, pp. 3481-3485, June 2004.

[14] P. Casari, M. Nati, C. Petrioli, and M. Zorzi, "Efficient Non-Planar Routing around Dead Ends in Sparse Topologies Using Random Forwarding," Proc. IEEE Int'l Conf. Comm. (ICC '07), pp. 3122-3129, June 2007.

[15] Park, Geon Yong, et al. "A Novel Cluster Head Selection Method based on K-Means Algorithm for Energy Efficient Wireless Sensor Network." *Advanced Information*

[16] Petrioli, Chiara, et al. "ALBA-R: Load-balancing geographic routing around connectivity holes in wireless sensor networks." *Parallel and Distributed Systems, IEEE Transactions on* 25.3 (2014): 529-539.

[17] Q. Fang, J. Gao, and L.J. Guibas, "Locating and Bypassing Holes in Sensor Networks," ACM Mobile Networks and Applications, vol. 11, no. 2, pp. 187-200, Apr. 2006.

[18] Q. Huang, S. Bhattacharya, C. Lu, and G.-C. Roman, "FAR: Face-Aware Routing for Mobicast in Large-Scale Networks," ACM Trans. Sensor Networks, vol. 1, no. 2, pp. 240-271, Nov. 2005.

[19] R. Fonseca, S. Ratnasamy, J. Zhao, C.T. Ee, D. Culler, S. Shenker, and I. Stoica, "Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets," Proc. Second Conf. Symp. Networked Systems Design and Implementation (NSDI '05), vol. 2, pp. 329-342, May 2005.

[20] S. Basagni, M. Nati, and C. Petrioli, "Localization Error-Resilient Geographic Routing for Wireless Sensor Networks," Proc. IEEE GLOBECOM, pp. 1-6, Nov./Dec. 2008.

[21] Shim, Young-Chul, and C. V. Ramamoorthy. "Monitoring and control of distributed systems." *Systems Integration, 1990. Systems Integration'90, Proceedings of the First International Conference on*. IEEE, 1990.

[22] Xu, Jiu-qiang, et al. "Study on WSN topology division and lifetime." *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on*. Vol. 1. IEEE, 2011.

[23] Y. Zhao, Q. Zhang, Y. Chen, and W. Zhu, "Hop ID Based Routing in Mobile Ad Hoc Networks," Proc. IEEE 13th Int'l Conf. Network Protocols (ICNP '05), pp. 179-190, Nov. 2005.

[24] Y.-J. Kim, R. Govindan, B. Karp, and S. Shenker, "On the Pitfalls of Geographic Routing," Proc. ACM Joint Workshop Foundations of Mobile Computing (DIALM-POMC '05), pp. 34-43, Sept. 2005.

[25] Z. Li, R. Li, Y. Wei, and T. Pei, "Survey of Localization Techniques in Wireless Sensor Networks," Information Technology J., vol. 9, pp. 1754-1757, Sept. 2010.