ISSN: 2321-7782 (Online)

Volume 2, Issue 9, September 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Securing Sensor Networks with Packet Hopping Mechanism

Heena Singh[1]
M.Tech Scholar, CSE Dept
JECRC University
Jaipur – India

Dr. Naveen Hemrajani[2]
Head of Department, CSE Dept
JECRC University
Jaipur – India

Abstract: Wireless networks are low-power actuator devices which are poised to turn out to be widely used in the commercial and military environments for the surveillance. Security problems for the wireless sensor networks have been exacerbated by the limited energy, power and the size of the sensor devices. In this research paper, the proposed work describes the design and implementation of the deployment of the sensor nodes, master node selection, and dissemination of the authenticated messages into the network to enhance the communication securely among them. Frequent updating of node information in the database that supports the secure communication under very limiting energy. In addition, it selects highly energetic shortest routes that have authenticated nodes for data transmission. Thus, the proposed work improves the performance of the sensor networks by exploiting multiple highly energetic shortest paths with authenticated routers.

Keywords: Wireless Sensor Networks, hopping mechanism, Energy Based Calculation, Performance, Authentication.

I. Introduction

Wireless sensor node has the capability of sensing, processing, along with the transmission. A sensor system is a deployment, that includes substantial numbers of minute, cost-effective, powered devices that can sense, compute, as well as communicate with different devices when it comes to gather the local data to create wide-spread decisions about a physical environment. WSNs are tends to be resource constrained as they're densely deployed. The number of nodes in WSNs will be placed beyond which will involving ad hoc networks. WSN system topology is consistently transforming, WSNs utilize broadcasting transmission mediums. The devices in these types of applications might be smaller or even huge, as well as the ad hoc networks might be "wired" or even instant i.e wireless. Due to the rigorous energy restrictions associated with large numbers of densely deployed sensor nodes, it requires some sort of selection associated with the network methodology to carry out a variety of network control along with supervision features for example node localization, synchronization along with network stability. The more common redirecting methods possess many shortcomings whenever given to WSNs, which might be generally because of the energy-constrained character.

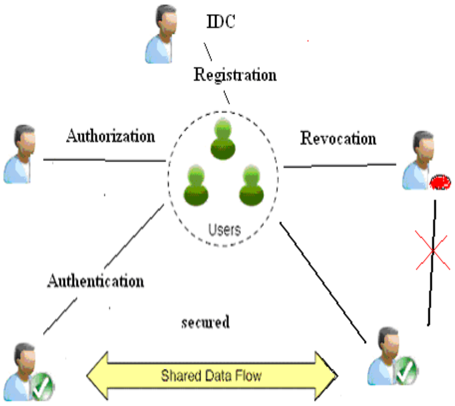


Fig1: Secure data communication

II. Proposed System

1. Detection based path hopping Technique works in three phases such as selection of master key, detection process and data forwarding. In this approach we will select number nodes we want to deploy. As the WSN are densely deployed so the number sensor nodes will vast. After the deployment of the nodes, in the first phase we will select a sender which is called as the “Master Node” and will be considered as an authenticated node from the network.
2. Second phase of the method is detection. In this master node (MN) will then send authentication detection message to all the nodes in the network. For authentication network key method is used where a single key is distributed all over the network. All the nodes will reply to the authentication detection message.
3. In the authentication reply they will send their network id and a Network key to master node. After all reply received from the master node; it will make a database of authenticated or good nodes and unauthenticated or malicious nodes. The next step after selecting the sender and receiver is data transmission phase. In this phase data transmission will take place between nodes. In the data transmission the sender will first calculate the shortest path in the direction to the receiver. This distance will be calculated by the sender by a formula called “distance formula”. Distance vector is method to calculate distance between two points in two dimension plane.

III. Methodology used

In this methodology we will choose number hubs we need to send. As the WSN are densely conveyed so the number sensor nodes will be expansive. After the sending the nodes, in the first stage we will choose a sender called "Expert Node" which will be considered as a confirmed node from the system. Second period of the strategy is identification. In this Master Node (MN) will then send confirmation discovery message to all the nodes in the system. For validation system key approach is utilized where a single key is disseminated everywhere throughout the system. All the nodes will answer to the verification recognition message.

IV. Energy Based Path Calculation

In sensor networks, if authenticated forwarding nodes (next hop) have low energy, may chances to make local topology inaccuracy. If the node involved in the shortest forwarding path has low energy, that node will not participate in the packet transmission because the node will be drop the packet. Hence it is required to select the nodes with high energy and reduce the packet loss in the network. Multiple highly energetic shortest paths are calculated to the sink node. This project with energy based forwarding node selection improves routing performance more than existing sensor routing protocol.

V. Performance Metrics

A. Packet Delivery Ratio

- PDR is the proportion to the total amount of packets reached the receiver and amount of packet sent by source. If the amount of malicious node increases, PDR decreases. The higher mobility of nodes causes PDR to decrease.

$$\text{PDR (\%)} = \frac{\text{Number of packets successfully delivered to destination}}{\text{Number of packets generated by source node}}$$

B. End-to-End Delay

- End-to-End delay is the time taken for a packet to reach the destination from the source node.

$$\text{End to End delay (ms)} = \sum \quad \begin{array}{l}\text{(Delay of each entities data packet)} \\ \text{Total number of delivered data packets}\end{array}$$

C. Energy Consumption

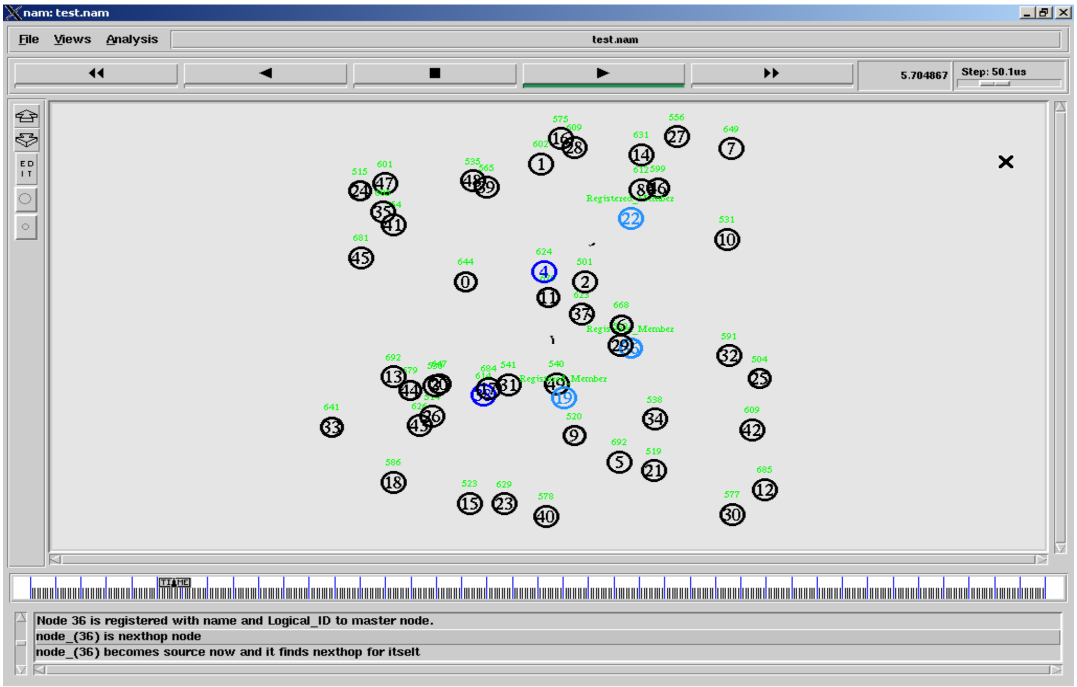
- Energy Consumption is total amount of energy consumed by all nodes in the network

VI. SIMULATION

Node 36 is registered with name and logical_Id to master node.

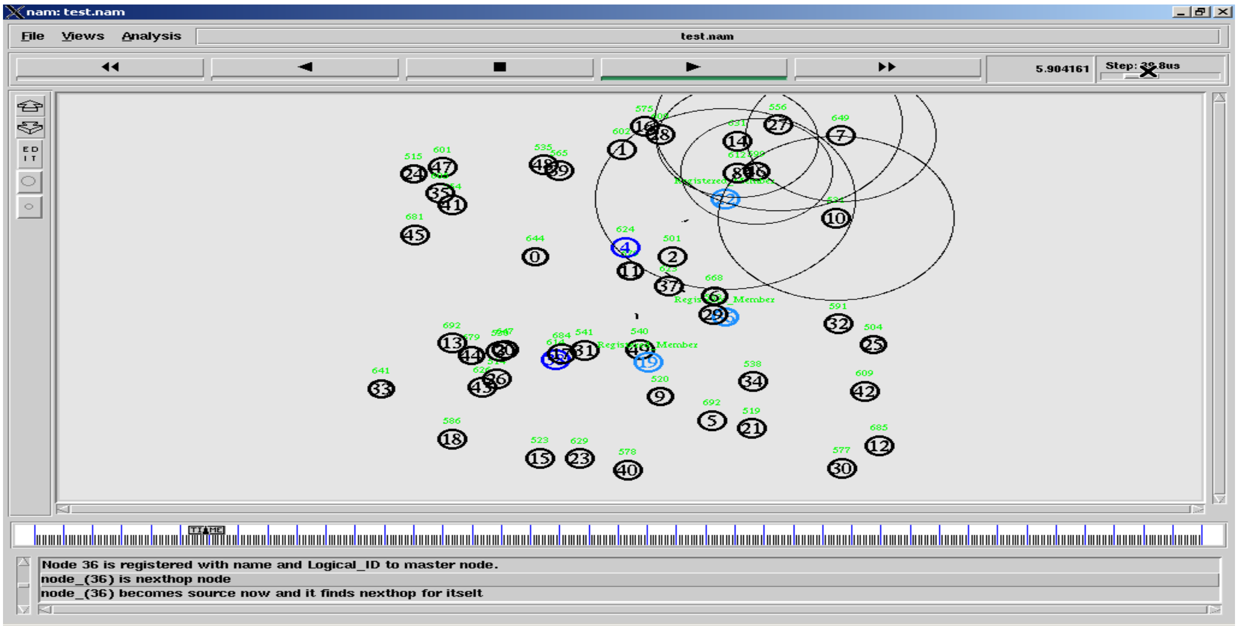
Node 36 is next hop node

Node 36 becomes source now and it finds nexthop for itself



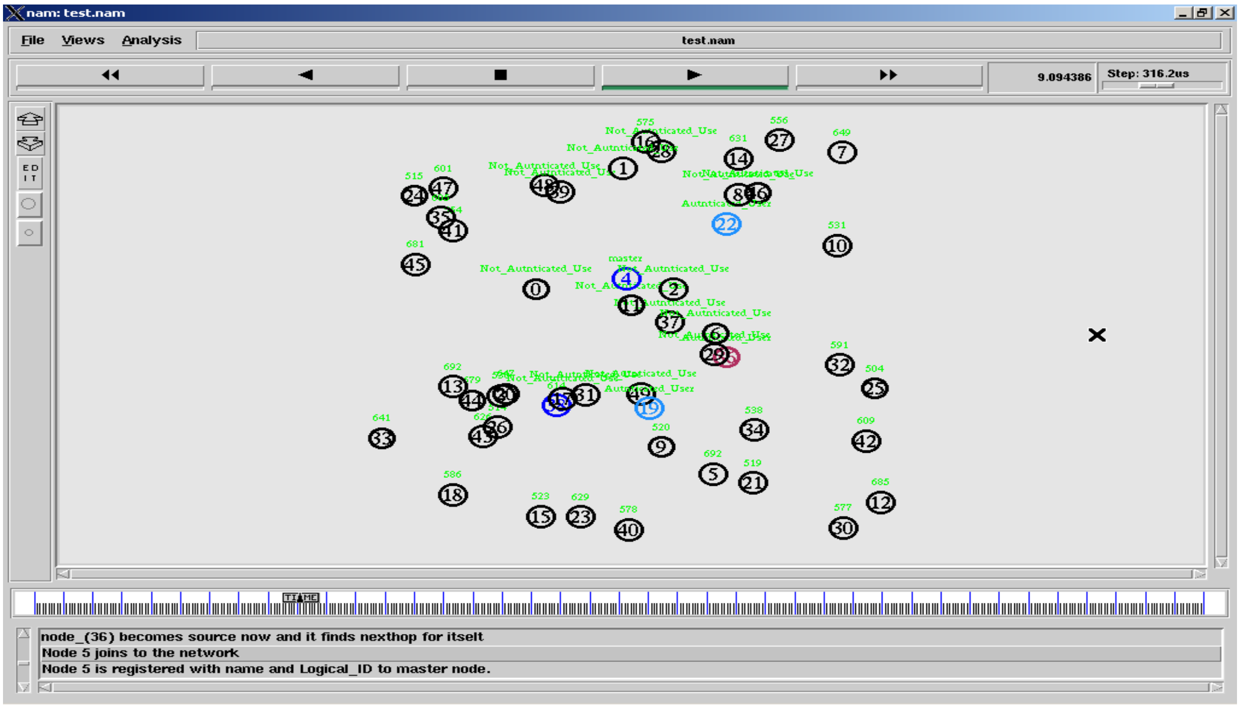
Node 36 is registered with name and Logical_ID to master node.
node_(36) is nexthop node
node_(36) becomes source now and it finds nexthop for itself

After received the authentication detection message from master node, neighbors will report the authenticated reply message to master node. Authentication reply message contains the network id and a Network key to master node.

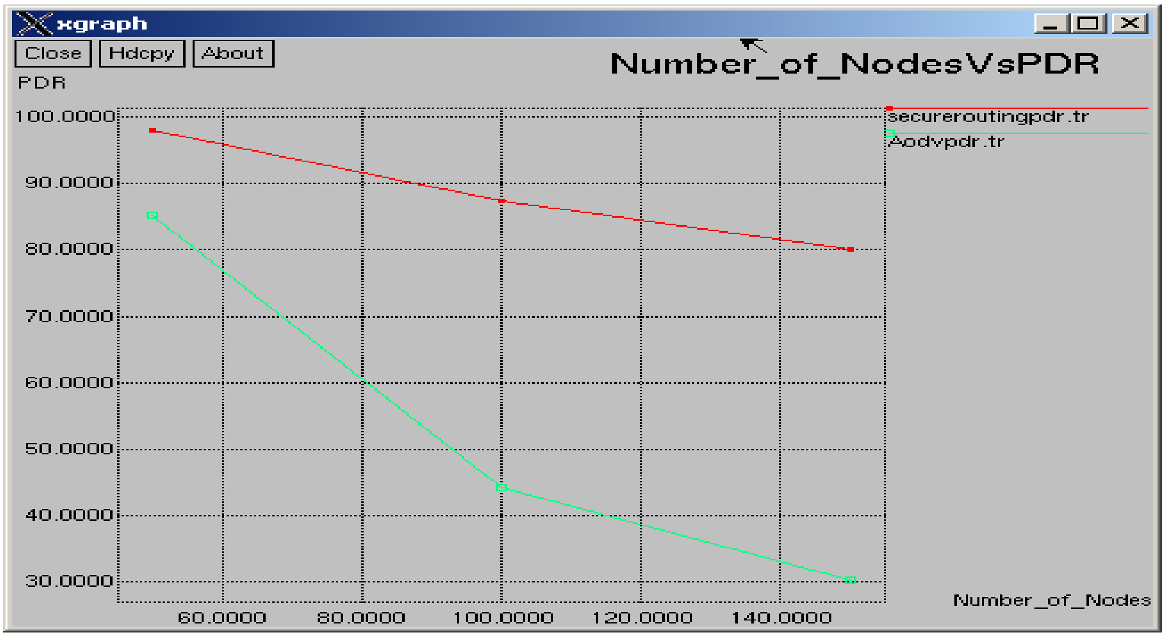


Node 36 is registered with name and Logical_ID to master node.
node_(36) is nexthop node
node_(36) becomes source now and it finds nexthop for itself

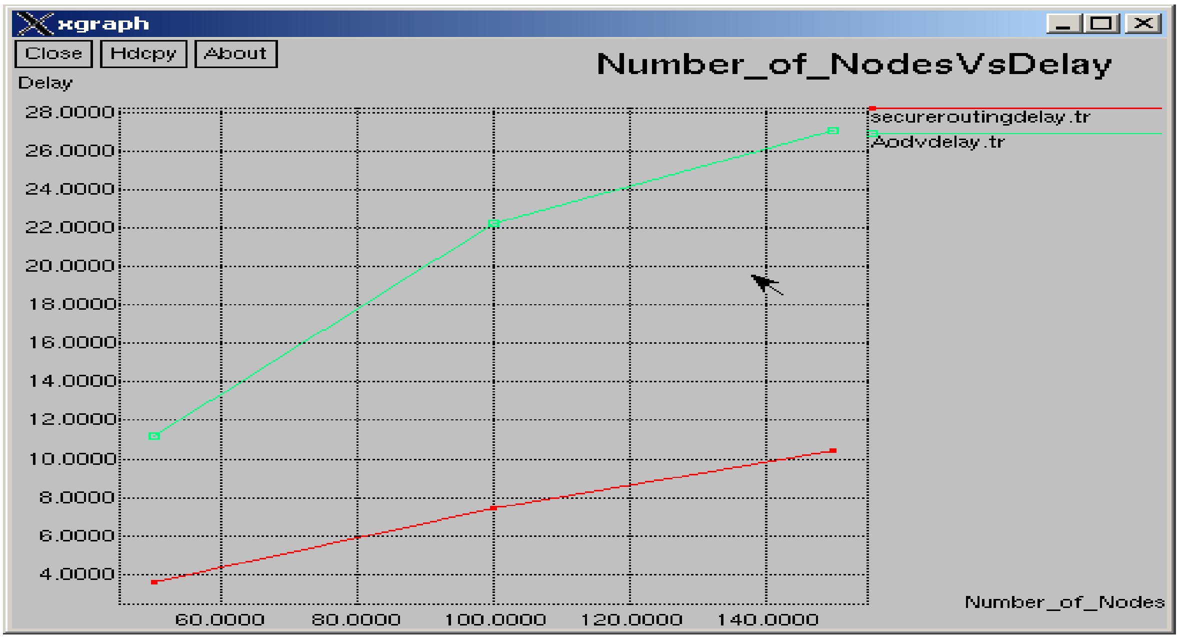
Energy is calculated for each node in the network. while choosing the router the energy of the node considered and that is router selected with the highest energy ,authenticated node selected for route the packet to the destination . Shortest path calculated with the consideration of energy of the nodes.



node_(36) becomes source now and it finds nexthop for itself
Node 5 joins to the network
Node 5 is registered with name and Logical_ID to master node.



This graph shows comparison between the number of nodes increases and the packet delivery ratio decreases in the network. Compare to the existing system the proposed system provides the high packet delivery ratio. Because it will send packet to the destination via authenticated node.



This graph shows comparison between number of nodes increases corresponding delay obtained in the network. Compare to the existing system the proposed system, it reduces the delay due to the selection of shortest path for data transmission

VII. Conclusion

The new making of sensor networks will deploy large numbers of low cost, low-power nodes. Contrary to widely held beliefs, our results indicate that the authentication and unauthentication message exchange protocols using optimized software implementations of public-key cryptography and are very viable on small wireless devices. This proposed system focuses on sustaining reliable routing and source authentication for the sensor network traffic. Depending on the frequency of authentication message computations, its relative energy cost may even be negligible. Furthermore, our analysis suggests that the use of shortest paths over WSN can lead to significant energy savings. In addition to the computational benefits of database including both authenticated and unauthenticated neighbors, its smaller authentication messages lead to significant savings in public-key communication costs.

References

1. R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, “A Spontaneous Ad-Hoc Network to Share WWW Access,” EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.
2. V. Kumar and M.L. Das, “Securing Wireless Sensor Networks with Public Key Techniques,” Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.
3. J. Goodman and A. Chandrakasan, “An Energy Efficient Reconfigurable Public-Key Cryptography Processor Architecture,” Proc. Int’l Workshop Cryptographic Hardware and Embedded Systems (CHES ’00), pp. 175-190, 2000.
4. A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Chang, “Energy Analysis for Public-Key Cryptography for Wireless Sensor Networks,” Proc. IEEE Third Int’l Conf. Pervasive Computing and Comm. (PerCom ’05), pp. 8-12, Mar. 2005.
5. V. Untz, M. Heusse, F. Rousseau, and A. Duda, “Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks,” Proc. First Ann. Int’l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous ’04), Aug. 2004.
6. S. Zhu, S. Xu, S. Setia, and S. Jajodia, “LHAP: A Lightweight Hopby- Hop Authentication Protocol For Ad-Hoc Networks,” Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.
7. A. Noack and S. Spitz, “Dynamic Threshold Cryptosystem without Group Manager,” Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.

AUTHOR(S) PROFILE

HEENA SINGH: Born in 1990 in Rajsamand District (Rajasthan). She completed her B.Tech. (Information Technology) from Rajasthan Technical University and currently pursuing M.Tech (Computer Science) from JECRC University. Her major fields of study areas are Information Security, Wireless Sensor Networks.

NAVEEN HEMRAJANI: Prof. (Dr.) Naveen Kumar Hemrajani has twenty years of research and teaching experience in Computer Engineering. He is currently a Professor and Head in Computer Science and Engineering Department, JECRC University. Presently he is chairman of computer Society of India, Jaipur Chapter. He is editorial member of various international journals of repute; more than 70 papers are credited to his credentials. Research Areas are Computer Networks and Software Engineering.