International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 5050 - 5053

Secure Data Collection Using Randomized Multipath Routing

Dr.M.Naga Ratna
Assistant Professor
Dept of Computer Science & Engineering
JNTUH College of Engineering Hyderabad
Email: mratnajntu@jntuh.ac.in

P.Vamsi priya
(M.Tech) Dept of computer science & engineering
JNTUH College of Engineering Hyderabad
priya.vamsi524@gmail.com

Abstract:-Wireless Sensor Networks (WSNs) are widely used in various real time applications such as surveillance, environment monitoring, studying wildlife habitat and so on. As the nodes in the network are resource constrained, they are vulnerable to various attacks. This is the reason there is need for secure data collection in such networks. Many solutions came into existence to provide secure communications in WSN. However, the solutions were based on different techniques. Minimization of packet failure rate is one of the objectives of many researchers in this area. The potential attacks on the network can jeopardise its purpose. Recently Alghamdi *et al*. proposed a solution using multipath routing in which the effect of adversaries is reduced besides ensuring secure data transmission in the presence of malicious nodes in the network. Our work is similar to this with certain improvements in terms of energy consumption and also packet delivery failure ratio. We implemented a WSN with simulations and our approach used a controller in the network which, in consultation with base station, can play a vital role in prevention of attacks. Since the solution is based on randomized multipath routing, it is able to withstand potential attacks and ensure that the failure of packet delivery is minimized and the overall network performance is improved. The simulation results reveal that the proposed approach has better performance in terms of performance level of protocol, network throughput, delay analysis, percentage of packet loss, and energy consumption.

Keywords: – *Wireless Sensor Network, multipath routing, secure data collection, data collection*

*****

I. INTRODUCTION

Wireless Sensor Network (WSN) is a network of sensor nodes connected to a base station. The sensor nodes in the network can capture data from surroundings or as per their intended purpose, and then they send the data to base station. The overall communication is many-to-one communication as all the sensor nodes send data to base station. As the sensor nodes have limited energy resources the transmission mechanism needs to be simplified. This needs to be motivated by the fact that by reducing energy consumption it is possible to increase lifetime of network. A typical WSN appears as shown in Figure 1. Sink node is also known as base station. The sensor networks are able to sense data or track target and send the data to sink node. Then it is possible to have this network integrated with Internet so that it is possible to enable Internet users also to have access to the data collected by WSN. This is the typical scenario in which WSN operates in order to monitor environments or capture data of the surroundings and send to base station.

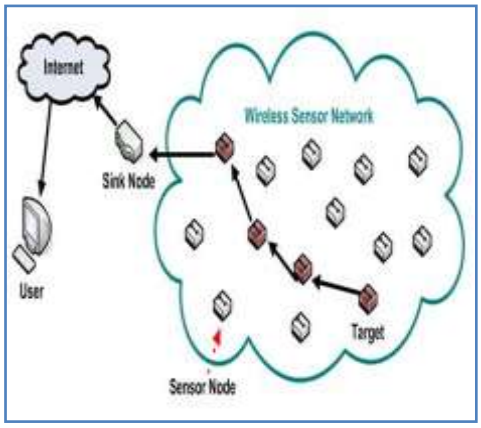

Figure 1 – A typical WSN

As can be seen in Figure 1, it is evident that the sensor nodes are able to communicate with base station either directly or through other sensor nodes. This kind of network is used in this paper for making simulation experiments. The network is considered with potential malicious nodes as well.

Due to the limitations in the WSN, the proposed security mechanism takes care of randomized multipath routing in order to thwart effect of attacks on the network. The proposed mechanism can withstand attacks and ensure that the packet delivery ratio is improved even in the presence of attacks. Our contributions in this paper are described here. We proposed a randomized multipath routing mechanism that ensures that data is transmitted to the base station with complete security. Moreover the data reaches base station without packet loss. The packet delivery ratio and energy consumption are improved. We made extensive simulations that reflect the efficiency of the proposed approach. The remainder of this paper is structured as follows. Section 2 provides review of literature. Section 3 presents the proposed solution. Section 4 presents experimental results while section 5 concludes the paper and throws light into future directions.

II. RELATED WORKS

This section reviews the relevant literature. The research on security of WSN has been around for number of years. Overhearing technique is used in [1] to prevent modification attack that will try to modify packets being delivered in the network. This technique was capable of examining packets and ensured that the packet modification attack was prevented. However, it is known that the solution is made at the cost of energy. To state differently, the overhearing technique consumes more energy as explored in [2]. Encryption and adding extra bit to packets was the solution

made in [3] where the packet modification attacks were effectively identified. The sensor node behaviour is studied and malicious nodes are identified. Multipath routing has been around for efficiently prevent attacks like selective forwarding and modification attacks as explored in [4], [5], [6] and [7]. There are different types of multipath routing such as node disjoint, link disjoint, and partially disjoint.

The improvement of transmission reliability was explored in [8]. Secure and reliable data collection also considered in [9] which is an extension to the research made in [8]. N-1 multipath routing is another model that was proposed in [10] for reliable packet delivery in WSN. Collision aware multipath routing with energy efficiency was proposed in [11]. It makes use of two collision-free paths in order to have increased packet delivery ratio. In [12] another solution is made which is energy efficient and low-interference multipath routing for WSNs. Direct diffusion algorithm was proposed in [13] for enabling multimedia services in WSN. Multiple node-disjoint paths were employed in [14] for load balancing and secure communications. Randomized multipath routes were also explored in [15] and [16] for energy efficiency and secure data transmission in WSNs. In this paper we proposed yet another approach that could improve the packet delivery ratio besides making the network more energy efficient.

III. PROPOSED SYSTEM

We proposed an approach in WSN that facilitates randomized multipath routing for secure data collection. It is essential to have security measures in place as WSN is vulnerable to various attacks due to resource scarcity and also the mobility of nodes. However, for our study we considered a static network where nodes do not move. The sensors are placed in a fixed place. Only one base station is considered for experiments. Sensor nodes can communicate with both base station and also neighbouring sensors. The communication process between sensors is bidirectional. The nodes are interconnected in such a way that every sensor node has a path to connect to base station. Sensor nodes are supposed to sense data from surroundings and the data then is sent to base stations either directly or through other sensor nodes. It does mean that each sensor node can act as receiver and transmitter. There is no concept of data aggregation while collecting data. We studied the problem of minimizing packet delivery failure rate. There are many existing approaches to handle this problem. In the existing solution the packet to be delivered is made three copies and sent to base station. Different paths are used randomly to send packets to the destination.

By using multipath routing, the packet delivery failure ratio was reduced. There are some problems with the existing system. The energy consumption is more. The throughput could be improved further. The malicious node identification could be improved and the overall security can be improved. Therefore it is possible to reduce the failure rate further. Towards this endeavour, in this paper, randomized multipath routing is considered to be one of the best solutions. By using efficient data transmission the energy consumption is reduced besides increasing life time of WSN. The behaviour of malicious nodes is identified with high accuracy. Hash technique is used for secure data transmission and identification of adversaries in the network. The WSN is used to make the experiments in the presence of multiple malicious nodes. The secure multipath routing approach used in this paper is robust to various attacks. The data transmission was proved to be secure even in the presence of potential malicious nodes in the network. The following equations are used to achieve the performance.

Energy Consumption

$$E_{SR}=\mathrm{P}(S)\beta e_{SR} = K(\alpha + \mu_{r2})$$

Packet Delivery Ratio

$$R_{i.j}=\frac{\Sigma_{k=1}^{n} x_{ik} x_{jk} - n_{xi} - xj -}{\left[\Sigma_{k=1}^{n} x_{ik}^2 - n_{xi}^2 -\right]^{1}/_{2}\left[\Sigma_{k=1}^{n} x_{jk}^2 - n_{xj}^2 -\right]^{1}/_{2}}$$

Packet Loss Rate

$$x[k+1] = Ax[k] + v[k]$$

$$\mathrm{s}= Cx[k][k] + e[k]$$

$$\mathrm{E}= \{(x[k] - x\hat{}[k])T (\boldsymbol{x}[\boldsymbol{k}] - \boldsymbol{x}\hat{}[\boldsymbol{k}])\}$$

Delay Time

$$D(n) = \theta\left(\frac{1}{\left(\frac{4}{tan\ 2\frac{\theta}{2}}\right)\frac{2}{\propto}\sqrt{a(n)}}\right)$$

Throughput

$$T(n) = \theta\left(\frac{1}{k_{2n\sqrt{a(n)}}}\right)$$

The implementation of the WSN and the experiments are described here. The NS2 simulations show the proposed approach. First of all a network is created with nodes whose position is fixed. The network contains one base station, one controller and many sensor nodes. There is communication between base station and nodes in the network. There is

ISSN: 2321-8169
5050 - 5053

coordinated effort between controller and base station in order to identify malicious nodes and also reduce packet delivery failures with the multipath routing chosen randomly. There is constant information exchange between base station and network controller with respect to randomized routing path and secure communications. Packet transmission is experiments through simulations through randomized multipath routing. From time to time energy levels of the nodes are considered to determine malicious nodes. Energy consumption of the network is also reduced due to the proposed approach. Data transmission is made securely using hash technique. Every time data is transmitted, the network controller validates it and the authentication is failed for malicious nodes which are denied from data transmission. Malicious nodes try to make attacks that are thwarted by the network. Controller plays a vital role in detection of adversaries.

IV. EXPERIMENTAL RESULTS

This section provides experimental results obtained through extensive simulations. Since the solution is based on randomized multipath routing, it is able to withstand potential attacks and ensure that the failure of packet delivery is minimized and the overall network performance is improved. The simulation results reveal that the proposed approach has better performance in terms of performance level of protocol, network throughput, delay analysis, percentage of packet loss, and energy consumption. The results are as shown below.

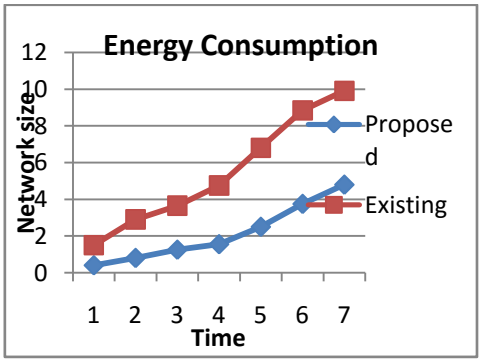

Figure 2 – Performance comparison in terms of energy consumption

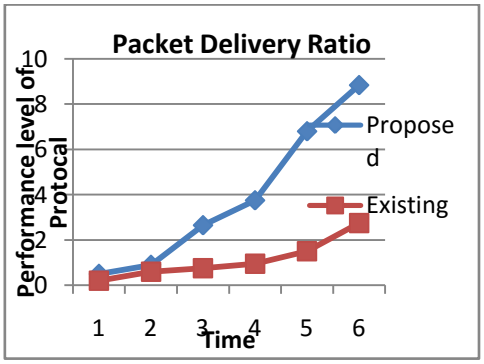

Figure 3 – Performance comparison in terms of packet delivery ratio

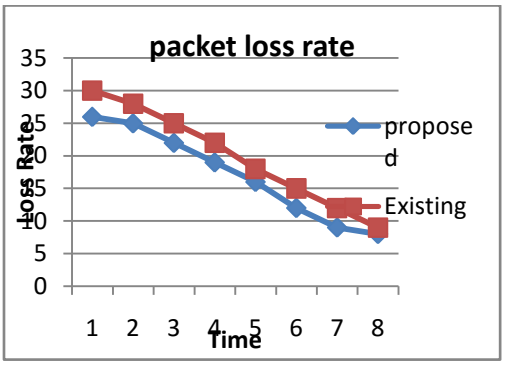

Figure 4 – Performance comparison in terms of packet loss rate

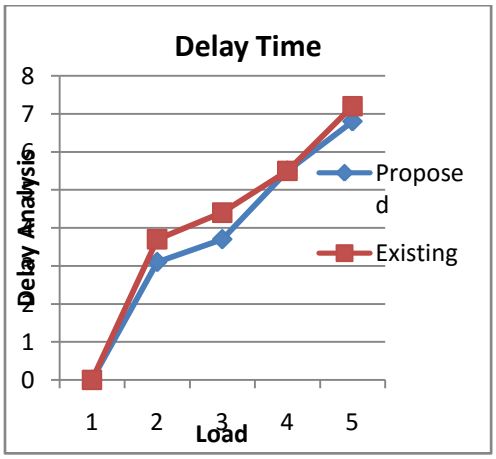

Figure 5 – Performance comparison in terms of delay analysis

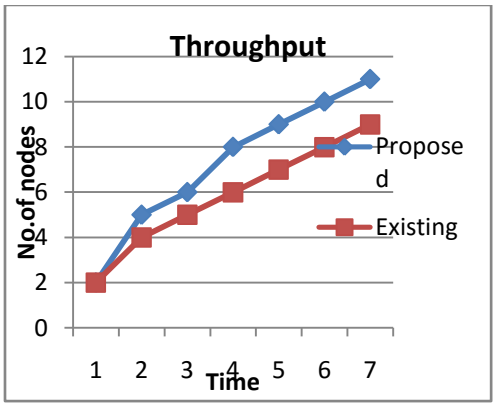

Figure 6 – Performance comparison in terms of throughput

As can be shown in Figure 2, 3, 4, 5, and 6 it is evident that the proposed system has performance improvement significantly. The reason behind this is that the randomized multipath routing and the energy efficient transmission approach were considered important in the simulations. There are performance improvements with respect to energy consumption, packet delivery ratio, packet loss rate, delay analysis and throughput.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we studied multipath routing in WSNs for secure data collection. Secure data collection without losing packets is vital for the genuine information in such networks. As the network is vulnerable to attacks, it is imperative to have security mechanisms in place. Since the network nodes might be compromised or to state differently there might be some malicious nodes in the network that cause problems to secure data transmission, a fool proof mechanism is required. Towards this end, we proposed an approach that makes use of randomized multipath routing in a static network where nodes and base station are fixed. Our solution also makes use of a controller who will involve in secure data transmission. The nodes in the network can have bidirectional communications among themselves. The sensor nodes can either communicate with base station directly or they can do it through other sensor nodes. There are malicious nodes in the network that try to make attacks. The proposed solution makes use of multiple randomized routes in order to send packets to withstand potential attacks. The coordination between controller and base station can help in curbing attacks besides improving secure communication in the network. The network lifetime increases with energy efficient data transfer. The simulation results reveal that the proposed approach has better performance in terms of performance level of protocol, network throughput, delay analysis, percentage of packet loss, and energy consumption. This research can be extended further by considering other mobile networks such as MANET and VANET.

REFERENCES

[1] K.-F. Ssu, C.-H. Chou, and L.-W. Cheng, "Using overhearing technique to detect malicious packet-modifying attacks in wireless sensor networks," *Computer Communications*, vol. 30, no. 11, pp. 2342–2352, 2007.

[2] B. Bates, A. Keating, and R. Kinicki, "Energy analysis of four wireless sensor network mac protocols," in *Wireless and Pervasive Computing (ISWPC), 2011 6th International Symposium on*. IEEE, 2011, pp. 1–6.

[3] C. Wang, T. Feng, J. Kim, G. Wang, and W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," in Sensor, Meshand Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on, vol. 23, no. 5. IEEE, 2012, pp. 835–843.

[4] S. Mohammadi and H. Jadidoleslamy, "A comparison of link layer attacks on wireless sensor networks," International journal on applications of graph theory in wireless ad hoc networks and sensor networks(GRAPH-HOC), vol. 3, no. 1, pp. 35–65, 2011.

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures," Ad hoc networks, vol. 1, no. 2, pp. 293– 315, 2003.

[6] S. K. Singh, M. Singh, and D. Singhtise, "A survey on network security and attack defense mechanism for wireless sensor networks," International Journal of Computer Trends and Technology, vol. 4, no. 2,pp. 1–9, 2011.

[7] J. Sen, "A survey on wireless sensor network security," International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 2, pp. 55–78, 2009.

[8] H. Hassanein and J. Luo, "Reliable energy aware routing in wireless sensor networks," in Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second IEEE Workshop on. IEEE, 2006, pp. 54–64.

[9] W. Lou and Y. Kwon, "H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," Vehicular Technology, IEEE Transactions on, vol. 55, no. 4, pp. 1320–1330, 2006.

[10] W. Lou, "An efficient n-to-1 multipath routing protocol in wireless sensor networks," in Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on. IEEE, 2005, pp. 672–680.

[11] Z. Wang, E. Bulut, and B. K. Szymanski, "Energy efficient collision aware multipath routing for wireless sensor networks," in Communications, 2009. ICC'09. IEEE International Conference on. IEEE, 2009, pp. 91–95.

[12] M. Radi, B. Dezfouli, S. A. Razak, and K. A. Bakar, "Liemro: a lowinterference energy-efficient multipath routing protocol for improving qos in event-based wireless sensor networks," in Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on. IEEE, 2010, pp. 551–557.

[13] S. Li, R. K. Neelisetti, C. Liu, and A. Lim, "Efficient multi-path protocol for wireless sensor networks," International Journal of Wireless and Mobile Networks, vol. 2, no. 1, pp. 110–130, 2010.

[14] Y. Ming Lu and V. WS Wong, "An energy-efficient multipath routing protocol for wireless sensor networks," International Journal of Communication Systems, vol. 20, no. 7, pp. 747–766, 2007.

[15] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on. IEEE, 2005, pp. 113–126.

[16] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," Mobile Computing, IEEE Transactions on, vol. 9, no. 7, pp. 941–954, 2010.