Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 12 (6): 593-597, 2012
ISSN 1812-5654 / DOI: 10.3923/jas.2012.593.597

Wireless Sensor Network (WSN): Routing Security, Reliability and Energy Efficiency

[1]Noor Zaman, [1]Low Tang Jung, [2]Fawaz Alsaade and [3]Turki Alghamdi
[1]Universiti of Teknologi, PETRONAS, Malaysia
[2]College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia
[3]College of Computer and Information System, Umm Al-Qura University, Saudi Arabia

Abstract: Wireless Sensor Networks (WSNs) differ from conventional network in deployment, application and working mechanism. Sensor networks are always resource constraint and small in size, computation and memory storage. In WSN, sensor nodes are normally distributed openly in harsh environment and have open access for inside and outside menaces which could adversely affect their proper functioning. These threats became the source for choking of resources and loss of energy. This study focused on operational and architectural challenges for handling secure, reliable routing in wireless sensor network and proposed new mechanisms to secure reliable energy efficient routing protocol. The proposed methods were based on adding secondary route and secondary gateway to the clustering network. The simulation results for the proposed methods showed that overall network energy efficiency increased by approximately 25% and the possible security threats decreased by about 41% when compared to the clustered network. The paper presented the motivation for the proposed approaches and details of the simulation tests.

Key words: WSN, security, reliability, energy efficient, gateway, WSN routing

INTRODUCTION

Wireless sensor network is different in nature as compared to the conventional network, where WSN does not support most of conventional network topologies. Its distribution is open in nature and normally has open access to the threats as well. Sensor networks consists more number of nodes due to its size and limited capabilities of memory, computation and energy. It is basically a resource constraint type of networks. It contains very low power batteries without charging facilities. The sensor nodes are placed for a variety of applications to monitor the real-world environment. They play key role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring, health and building security monitoring (Capkun and Hubaux, 2006; Estrin *et al*., 1999; Wang *et al*., 2005; Zaman and Abdullah, 2010). Mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc., are a challenging task with sensor networks. While unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes. However, nodes cannot be assumed trustworthy due to the decentralized nature of the network and the absence of any infrastructure. Many researchers tried to build a sensor trust model to solve the problems which are beyond the capabilities of traditional cryptographic mechanisms (Yan *et al*., 2003; Ren *et al*., 2004; Zhang *et al*., 2009; Sharma *et al*., 2010). As the sensor nodes, in most cases, are unattended and physically insecure, vulnerability to physical attack is an important issue in WSNs. A number of prepositions exist in the literature for defense against physical attack on sensor nodes (Sharma *et al*., 2010; Zaman *et al*., 2011). Wireless sensor networks research identified mainly the three key research areas as that of Dolev-Yao model "security and reliability", "routing and transport" and "in-network processing" for developing secure and reliable WSNs as described by Westhoff *et al*. (2006) in Fig. 1.

SIMULATIONS

Tested topologies and scenarios: The proposed system was tested through different simulation tests. Network Simulator 2 (NS-2) was used for simulation purpose. Initially, these simulation tests were conducted under two well-known scenarios (Fig. 2). In the first scenario, the simulation tests were conducted through random distribution of the network where data collection was done in tree structure (Fig. 2a). While cluster mechanism was used in the second scenario. In the cluster mechanism scenario, the network was divided into sub-networks. After that each sub-network or cluster collected

Corresponding Author: Fawaz Alsaade, College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia

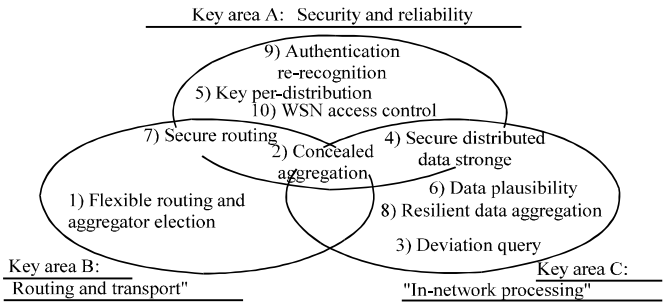

Fig. 1: Dolev-Yao wireless sensor network security model (Westhoff *et al*., 2006)

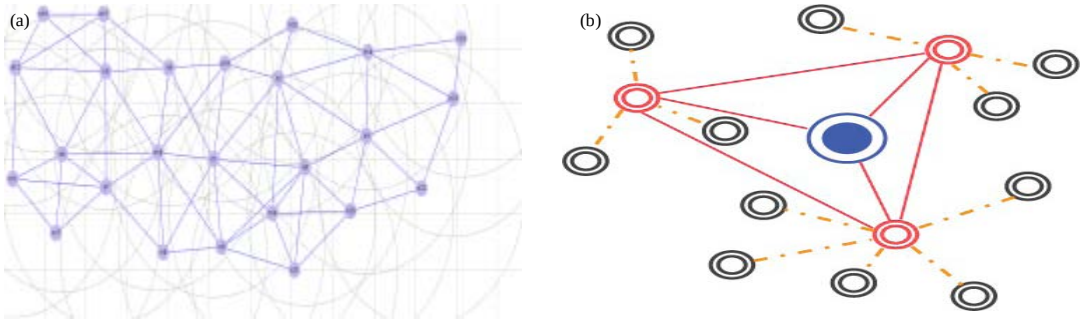

Fig. 2(a-b): (a) Normal distribution and (b) Cluster based node formation

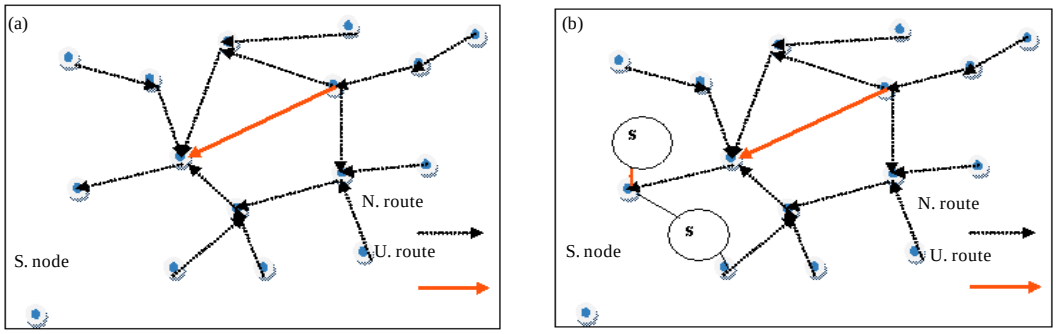

Fig. 3(a-b): (a) Clustered network with secondary routs and (b) Clustered network with secondary routs and secondary gateway

the data through one cluster head. Such data was then transferred to the gateway or the sink (Fig. 2b).

This paper studied two approaches for allowing data flow, inside a clustered network, smoother as well as reducing the chances of possible attacks. The first approach was based on adding secondary route to the clustered network. In second approach, the paper proposed to add both the secondary route and secondary gateway to the clustered network. The use of clustered network was based on the findings of earlier studies which reported it as one of the most effective methods for data transferring inside a network (Cao *et al*., 2007; Loscri *et al*., 2005). Since the process of data transfer was based on adding secondary route and secondary gateway to the clustered network, the two approaches were named Clustered Network with Secondary Route (CNSR) and Clustered Network with Secondary Route and Secondary Gateway (CNSRSG). The proposed approaches CNSR and CNSRSG are illustrated in Fig. 3a and b, respectively. It should be emphasized that the added secondary route

Table 1: Simulation parameters

Network area	200 m×200 rm or 400 m×400 rm
No. of sensor	100 or 400
Sensor distribution	Uniform random
Location of sink	Center of area
Radio range	40 m
MAC layer	IEEE 802.11
Unusual event sources	4
Routine data sources probability	P
Failure rate	f
Time-out constant (ξ)	1/T
Delay for retransmission M	0.02 sec
Data rate of unusual events	λU
Data rate of routine data	λR

and secondary gateway have different functionalities and are not for normal use. For example, the secondary route path became active to avoid congestion, in case any unusual event occurs at any time and helped to avoid the possible chances of threats by smoothing the network. On the other hand, secondary gateway becomes active in case the primary gateway was not responding due to loss of its energy after a certain period of time or any other issue. In that case, the secondary gateway continues the data transfer process after a bit delay and utilizes the energy of sensor nodes up to its last limit. Therefore, it is believed that the above proposed two approaches could help to enhance the data transfer process inside the network as well as reduce the possible number of security threat as compared to both the random distributed and clustered networks.

Simulation parameters: The Standard Simulation Parameters (SSP) are presented in Table 1.

RESULTS AND DISCUSSION

Since, the main objective of this study was to obtain an enhanced data transfer process inside a network with least possible number of security threats. The simulation tests were initially conducted under two different scenarios i.e. random distribution network and the clustering network. (1) The simulation tests provided a comparison between these two scenarios and (2) The simulation tests were applied to check the reliability and security for the proposed approaches (CNSR and CNSRSG) and then compared them to the clustering network. The network, in these sub sections, was distributed over an area of 200×200 m.

Random distribution network versus clustered network: As stated earlier, in case of random distribution network, the data was collected in tree structure. While for the cluster formation network, the data collection process was changed and formatted as clusters and cluster heads. The

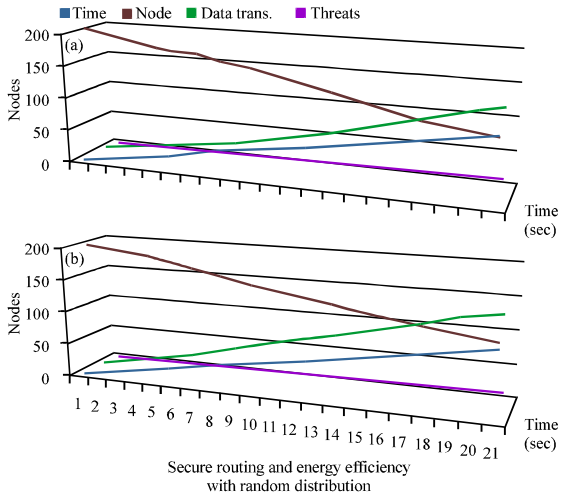

Fig. 4(a-b): Simulation results with both simple tree structure and cluster formation

simulation results showed that a significant improvement is obtained when the network nodes were distributed in the cluster formation (Fig. 4a, b). The results for the random distribution network are presented in Fig. 4a. On the other hand, Data in Fig. 4b illustrates the results when the network distribution was formed in cluster based mechanism. By comparing the results of security, reliability and energy efficiency for the random distribution network (Fig. 4b) with the corresponding results for the clustering distribution network (Fig. 4a), it was evident that better performance can be obtained with the latter. The study results are in agreement with the results of Cao *et al.* (2007), Younis *et al.* (2002), Patel *et al.* (2011) and Loscri *et al.* (2005) who reported that the most appropriate and effective approach to transfer data inside a network was obtained through the use of cluster network. Also, such type of network considerably reduced the possible number of security threats.

Proposed clustered network with secondary route (CNSR): In this case, the data gathering and working mechanism of sensor nodes was changed from normal routing path to additional secondary routing path (Fig. 3a). As stated earlier, this secondary routing path becomes active to avoid congestion, in case any unusual events occur during data transmission time and helps avoid the possible chances of threats by smoothing the network. Data in Fig. 5a shows the results for the proposed CNSR. An important outcome of the simulation tests can be observed by considering the results in Fig. 4b together with those in Fig. 5a. Based on these

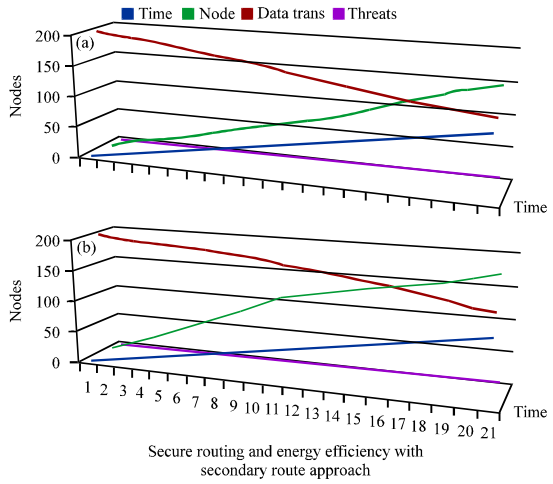

Fig. 5(a-b): Simulation results using, (a) CNSR and (b) CNSRSG approaches

results, it is clear that the proposed CNSR outperformed the clustered network in all aspects i.e. security, reliability and energy efficiency. The results, in Fig. 5a showed that there was approximately 20% increase in overall energy efficiency and 30% decrease in possible security threats as compared to the results obtained by the cluster network (Fig. 4b). Similar findings were reported by many researchers who proposed various security schemes which optimized these networks with resource metrics only. A number of secure and efficient routing protocols (Estrin *et al*., 1999; Zaman and Abdullah, 2011a, b) and secure data aggregation protocols were also proposed (Ye *et al*., 2004; Cao *et al*., 2007; Wood and Stankovic, 2008; Chan *et al*., 2003; Zaman *et al*., 2011).

Proposed clustered network with secondary route and secondary gateway (CNSRSG): In this case, an additional Sink 'S' or Gateway 'G' was added to the proposed method in the previous section (Fig. 3b). In other words, a secondary gateway along with the secondary routing path were simultaneously added into the cluster network. This secondary gateway continued the data transfer process even if the primary gateway is not responding due to loss of its energy. The results of security, reliability and energy efficiency obtained by the proposed method (CNSRSG) are presented in Fig. 5b. Some important outcomes of the simulation tests were observed by considering the aforementioned results (Fig. 4a, b, 5a, b). From these results, it is clear that using CNSRSG showed considerable improvement in the energy efficiency, data rate and in the possible security threats when compared to the other proposed method (CNSR). There was approximately 5% increase in overall energy efficiency and 11% decrease in possible security threats when CNSRSG was compared with the CNSR method.

Furthermore, a comparison of the results of security, reliability and energy efficiency for the cluster formation network (Fig. 4b) with the proposed method CNSRSG (Fig. 5b), it was evident that better performance can be obtained with the latter (CNSRSG method). Using CNSRSG resulted in approximately 25% increase in overall network energy efficiency and 41% decrease in possible security threats when compared to the clustering distribution network. This could be due to the individual capabilities provided by secondary route as well as secondary gateway; where the secondary route path helps avoid congestion, in case any unusual event occurred during data transmission time. It also reduced the possible chances of threats by smoothing the network. On the other hand, secondary gateway was in-charge to continue the data transfer process in case the primary gateway is not responding due to loss of its energy.

CONCLUSIONS

In general, the security, reliability and energy efficiency are the major concerns with Wireless Sensor Networks (WSNs). The security, reliability and energy solutions currently available for conventional networks cannot be applied with wireless sensor networks, because this type of network is resource constraint and small in size, computation and memory storage. Sensor nodes are normally distributed openly in harsh environment and have open access for inside and outside menaces, that can adversely affect their proper functioning. These threats are the main causes for choking of resources and the loss of energy.

This study has proposed two approaches namely Clustered Network with Secondary Route (CNSR) and Clustered Network with Secondary Route and Secondary Gateway (CNSRSG) to make the data flow, inside a WSN, smoother and to reduce the chances of the possible attacks. The simulation test results showed that using either CNSR or CNSRSG can significantly improve all aspects of security, reliability and energy efficiency of the Wireless Sensor Networks (WSN). This was clearly observed when using the CNSRSG approach. As a result, an approximately 25% increase in overall network energy efficiency and 41% decrease in possible security threats were obtained as compared to the cluster distribution network. The possible for this could be related to the individual capabilities provided by secondary route as well as secondary gateway; where the secondary route path helps avoid congestion, in case any unusual event

occurred during data transmission time. It also reduced the possible chances of the threats by smoothing the network, while the secondary gateway continued the data transfer process in case the primary gateway is not responding due to loss of its energy.

REFERENCES

Cao, Q., T. Abdelzaher, T. He and R. Kravets, 2007. Cluster-Based forwarding for reliable end-to-end delivery in wireless sensor networks. Proceedings of the IEEE INFOCOM 2007 26th IEEE International Conference on Computer Communications, May 6-12, 2007, IEEE Anchorage, USA., pp: 1928-1936.

Capkun, S. and J.P. Hubaux, 2006. Secure positioning in wireless networks. IEEE J. Sel. Areas Commun., 24: 221-232.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 11-14, 2003, Berkeley, CA, pp: 197-213.

Estrin, D., R. Govindan, J. Heidemann S. Kumar, 1999. Next century challenges: Scalable coordination in sensor networks. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 15-19, 1999, Seattle, Washington, USA., pp: 263-270.

Loscri, V., G. Morabito and S. Marano, 2005. A two-levels hierarchy for low-energy adaptive clustering hierarchy (TL-LEACH). IEEE Veh. Technol. Conf., 3: 1809-1813.

Patel, R., S. Pariyani and V. Ukani, 2011. Energy and throughput analysis of hierarchical routing protocol (LEACH) for wireless sensor network. Int. J. Comput. Appl., 20: 32-36.

Ren, K., T. Li, Z. Wan, F. Bao, R.H. Deng and K. Kim, 2004. Highly reliable trust establishment scheme in ad hoc networks. Comput. Networks, 45: 687-699.

Sharma, K., M.K. Ghose, D. Kumar, R.P.K. Singh and V.K. Pandey, 2010. A comparative study of various security approaches used in wireless sensor networks. Int. J. Adv. Sci. Technol., 17: 31-43.

Wang, X., W. Gu, S. Chellappan, D. Xuan and T.H. Laii, 2005. Search-based physical attacks in sensor networks: Modeling and defense: Technical report. Department of Computer Science and Engineering, Ohio State University.

Westhoff, D., J. Girao and A. Sarma, 2006. Security solutions for wireless sensor networks. NEC Techn. J., 1: 106-111.

Wood, A.D. and J.A. Stankovic, 2008. Security of Distributed, Ubiquitous, and Embedded Computing Platforms. In: Wiley Handbook of Science and Technology for Homeland Security, Voeller, J.G. (Ed.). John Wiley and Sons, Hoboken, USA.

Yan, Z., P. Zhang and T. Virtanen, 2003. Trust evaluation based security solution in ad hoc networks. Proceedings of the 7th Nordic Workshop on Secure IT Systems, September, 2003, Norway, USA..

Ye, F., L.H. Luo and S. Lu, 2004. Statistical en-route detection and filtering of injected false data in sensor networks. Proceedings of IEEE INFOCOM, March, 7-11, 2004, Hong Kong, China.

Younis, M., M. Youssef and K. Arisha, 2002. Energy: Aware routing in cluster-based sensor networks. Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, October 11-16, 2002, Texas, USA, pp: 129-136.

Zaman, N. and A. Abdullah, 2010. Energy efficient routing in wireless sensor network: Research issues and challenges. Proceedings of the International Conference on Intelligence and Information Technology, August, 2010, UK., pp: 1-6.

Zaman, N. and A. Abdullah, 2011a. Different techniques towards enhancing Wireless Sensor Network (WSN) routing energy efficiency and Quality of Service (QoS). World Applied Sci. J., 13: 798-805.

Zaman, N. and A. Abdullah, 2011b. Position Responsive Routing Protocol (PRRP). Proceedings of the 13th International Conference on Advance Communication Technology ICACT, February 13-16, 2011, IEEE., Korea, pp: 1-631.

Zaman, N., A. Abdullah, I. Ahmed and M. Ahmed, 2011. Routing energy efficiency and Quality of Service (QoS) of Wireless Sensor Network (WSN). Multi. Inform. J., 14: 3297-3304.

Zhang, Y., J. Zheng and H. Hu, 2009. Security in Wireless Sensor Networks. CRC Press, USA.