A Survey on Various Issues in Wireless Sensor Networks

Dr. K. H. Wandra, Sharnil Pandya

Abstract— Recent developments in micro-electro-mechanical systems (MEMS), wireless communications, and digital electronics have enabled development of low cost, low power, multifunctional sensor nodes are small and freedom to communicate in short distances. However, it has still remained an open challenge to deploy sensor nodes in wireless environment as we have to deal with innumerable constraints for their complete implementation. In this paper, a detailed survey has been carried out to analyze various techniques, which could be used to address present unresolved issues in wireless sensor networks.

Index Terms— Mobility and topology changes, Energy Backup, Physical Distribution, Localization, Data Aggregation, Fixed Communication Infrastructure, Strict Event Scheduling

1 Introduction

Recent trends in digital electronics and wireless communications have enabled the development of energy, low-cost and multifunctional sensor nodes which are small in size and have the freedom to communicate over short distances. These tiny sensor nodes, which consist of sensors, data processing components and communication, leverage the basic idea of sensor networks collective effort by a large number of nodes. Sensor networks have shown strong improvement as compared to the sensors, which have been developed in the past [32].

However, security is still a critical factor for their complete implementation. In this paper, we have discussed few WSN challenges, analyzed numerous security algorithms, techniques, frameworks and prepare a detailed study report based on various security issues exist in wireless sensor networks.

2 Overviews of Issues in Wireless Sensor Networks

2.1 Challenges and Properties of WSN Implementation

Various WSN challenges and properties are described as follows:

2.1.1 Lack of Fixed Communication Infrastructure

In WSNs, constant communication infrastructure does not exist. Thus, there exist some restrictions on the communication channel between the sensor nodes which may cause problems like unreliable communication [26]. However, it provides the broadcast advantage: A packet that has been transmitted by one sensor node to the neighbouring sensor node can also be received by all the other sensor nodes deployed in WSN.

2.1.2 Energy Backup

In general, sensor nodes used in establishing WSNs have energy limitations. So it is a big challenge to maintain and recharge sensor nodes after they have been deployed in wireless environments. In addition to this, various communication tasks also has high power requirements so it is difficult to reduce the sensor consumption ratio as well. To ensure long-term sensing operation and life span of WSN, communication links between sensor nodes must be analyzed and updated frequently [5].

2.1.3 Mobility Challenges and Changing Topologies

WSNs may involve dynamic scenarios in terms of drastic changes in topologies and mobility. In WSNs, during the deployment, new sensor nodes may join the network, and the existing nodes may be released or move through the network or out of the network. In such cases, nodes may stop functioning and surviving nodes may go in or out of the transmission radii of other nodes [26]. To ensure protection against attacks like node failure and dynamic topology WSNs must be robust.

2.1.4 Physical Distribution Constraints

WSNs contains a large number of tiny, inexpensive, disposable and autonomous sensor nodes that can initiate or establish communication links via transmission of sensory information [32]. In WSNs, data is distributed throughout the nodes in the network and can be gathered at a central station called base station(s) only with high communication costs. Therefore, the algorithms that require sensory information of the entire network become very expensive to deal with. To resolve this issue, various distributed algorithms are desirable [26]. Here data are distributed among the network nodes and can be collected at a central station with only high communication costs.

3 Outcomes of a Survey (Study Report)

This section provides a brief description of the major WSN challenges that can be reduced or addressed by following techniques that are described as follows[1-39]:

- *Dr. K. H. Wandra is a PhD guide for the taken research area. He is currently working as Director Academic at C. U Shah College of En-gineering, Wadhwan, India. PH-9825019080. E-mail: khwandra@yahoo.com*
- *Co-Author Sharnil Pandya is a research scholar in the area of sensor networks atR K University,Rajkot, India & also currently working as Asst. professor, Nirma University,Ahmedabad, India, PH-+91-9429130543. E-mail: sharnil.pandya@nirmauni.ac.in.*

3.1 Geometric Aware Routing

Geometric aware routing can be referred as a creation of location awareness of sensor nodes that are deployed in WSNs. Gathered location information is used to detect recorded events, or to send packets using different localization routing techniques. Moreover, location itself is often the data that needs to be sensed. Besides, we can also consider location itself as the data that needs to be sensed. Geometric techniques that use arrival time of signals from multiple base stations (storage stations) are commonly used in WSNs. Different examples of localization systems for WSNs is are presented in the sub-section [19].

3.2 Strict Event Scheduling

To save energy, most of the unused sensor nodes are being kept in standby most of the time, and can move into active mode periodically in order to send and receive sensory data. A rigorous program will be followed up when a node needs to wake up, the feeling, the transmission (or the execution of the movement), ensuring maximum network. This will force WSN nodes to take the right actions at the right time which is the main objective of scheduling WSN events [32].

3.3 Wireless Sensor Network Design and Deployment

Nowadays WSNs are used in numerous diversified applications ranging from patient monitoring thorough implanted sensors to monitoring forest fire through air-dropped sensors or sensors which can increment or decrement counter values. In most of the WSN applications, the sensor nodes need to be placed accurately at fixed or pre-determined locations, whereas in others, such positioning is not needed or none of use. So most of the sensor network design aims at determining the type, price and appropriate location of sensor nodes which could be placed in wireless environment in order to get a complete knowledge of its deployments [18].

3.4 Energy Conservation Using Energy Aware Routing Methods

As we all know, till date we don't have a satisfying solution of sensor's power backup requirements, so economic usage of energy is really critical. In many applications, longer network life is desired. To achieve this objective, we can use various proactive or reactive routing methods which can determine a path for a message from a source node to a destination node. As far as proactive routing methods are concerned, routing tables are being created for all routes and are stored regardless of knowledge of their use. In reactive routing methods, routes are computed as their need will get arise. In WSNs which have been deployed already, such routing tables have high memory requirements, and therefore, hybrids or combinations of proactive and reactive methods could be utilized to resolve such issues. Another possible solution to energy aware routing could be clustering which will cluster the network into hierarchies. Detailed description of an overview of modern WSN routing algorithms is highlighted in [6].

3.5 Data collection Using Aggregation Methods

Data Aggregation can be defined as the process of gathering data from different sources like sensors, cluster heads and external networks. To achieve this, we can use clustering techniques which can mitigate communication overhead of sending individual sensor readings to the base station(s). Nowadays WSNs are deployed in large-scale and voluminous data is generated. So to handle and maintain collection of such data is a critical issue [14]. Most widely used methods for data collection includes Kalman filter, Bayesian networks etc.

3.5 Management of Quality of Service Requirements

In general, QOS refers to efficient transmission of traffic between sensor nodes with specific requirements. QoS is a major issue in efficient WSNs deployment; it also has numerous meanings and perspectives. QoS is accepted as a ratio of measurement of the service quality of transmission and receiving of data between the sensor nodes. QoS is highly desirable in order to mitigate transmission problems like packet loss, bandwidth and fairness, delay and jitter between diverse sensor nodes. To achieve the goal of QoS, the network is required to analyze numerous wireless application requirements and implement few QoS mechanisms in WSNs [6].

3.7 High Level Security

Sensor nodes in WSNs are susceptible to innumerable security attacks like eavesdropping, impersonating, message distorting etc. Due to this, such security attacks can affect poorly protected sensor nodes in a negative way in terms of information theft or loss. It is really difficult to protect such sensor nodes due to dynamic topology. Various security challenges in wireless sensor networks are analyzed and critical issues that need to be resolved for achieving such high level security are described in [1].

4 Conclusion

In this paper we have discussed, reviewed and analyzed numerous wireless challenges that have still remained unresolved till date. In addition to this, we have also tried to address these wireless challenges by proposing certain techniques or solutions. These techniques could play an important role in achieving desired results.

5 Acknowledgements

At last but not least, we would like to appreciate all the people who help us directly or indirectly in preparing this survey paper

References

[1] Modares, Hero; Salleh, Rosli; Moravejosharieh, Amirhossein; , "Overview of Security Issues in Wireless Sensor Networks," Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on , vol., no., pp.308-311, 20-22 Sept. 2011.

[2] Xiaowang Guo; Jianyong Zhu; , "Research on security issues in Wireless Sensor Networks," Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on , vol.2, no., pp.636-639, 12-14 Aug. 2011.

[3] HongShan Qu; Wen Liu; , "A robust key predistribution scheme for wireless

sensor networks,"Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.634-637, 27-29 May 2011.

[4] Wang Hai-Chun; Huang Tao; , "Design of Security Gateway Based on Chaotic Encryption," Internet Technology and Applications (iTAP), 2011 International Conference on , vol., no., pp.1-4, 16-18 Aug. 2011.

[5] Burgner, D.E.; Wahsheh, L.A.; , "Security of Wireless Sensor Networks," Information Technology: New Generations (ITNG), 2011 Eighth International Conference on , vol., no., pp.315-320, 11-13 April 2011.

[6] Vithya, G.; Vinayagasundaram, B.; , "Actuation sensor with adaptive routing and QOS aware checkpoint arrangement on Wireless Multimedia Sensor Network," Recent Trends in Information Technology (ICRTIT), 2011 International Conference on , vol., no., pp.444-449, 3-5 June 2011.

[7] Akerberg, J.; Gidlund, M.; Bjorkman, M.; , "Future research challenges in wireless sensor and actuator networks targeting industrial automation," Industrial Informatics (INDIN), 2011 9th IEEE International Conference on , vol., no., pp.410-415, 26-29 July 2011.

[8] Sahana, A.; Misra, I.S.; , "Implementation of RSA security protocol for sensor network security: Design and network lifetime analysis," Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on , vol., no., pp.1-5, Feb. 28 2011-March 3 2011.

[9] Junqi Duan; Yajuan Qin; Sidong Zhang; Tao Zheng; Hongke Zhang; , "Issues of Trust Management for Mobile Wireless Sensor Networks," Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on , vol., no., pp.1-4, 23-25 Sept. 2011.

[10] Sheela, D.; Priyadarshini; Mahadevan, G.; , "Efficient approach to detect clone attacks in Wireless sensor etworks," Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.5, no., pp.194-198, 8-10 April 2011.

[11] Ullah, F.; Ahmad, M.; Habib, M.; Muhammad, J.; , "Analysis of security protocols for Wireless Sensor Networks," Computer Research and Development (ICCRD), 2011 3rd International Conference on , vol.2, no., pp.383-387, 11-13 March 2011.

[12] Iram, R.; Sheikh, M.I.; Jabbar, S.; Minhas, A.A.; , "Computational intelligence based optimization in wireless sensor network," Information and Communication Technologies (ICICT), 2011 International Conference on , vol., no., pp.1-6, 23-24 July 2011.

[13] Ning, H.; Liu, H.; Mao, J.; Zhang, Y.; , "Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems," Communications, IET , vol.5, no.12, pp.1755-1768, August 2011.

[14] Yang, Piyi; Cao, Zhenfu; Dong, Xiaolei; Zia, Tanveer A.; , "An Efficient Privacy Preserving Data Aggregation Scheme with Constant Communication Overheads for Wireless Sensor Networks," Communications Letters, IEEE , vol.15, no.11, pp.1205-1207, November 2011.

[15] Fan Wu; Hao-Ting Pai; Xinxin Zhu; Pei-Yun Hsueh; Ya-Han Hu; , "Dynamic access control for secure group communication in wireless sensor networks," Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2011 8th International Conference on , vol., no., pp.288-291, 17-19 May 2011.

[16] Bechkit, W.; , "New key management schemes for resource constrained wireless sensor networks," World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a , vol., no., pp.1-3, 20-24 June 2011.

[17] Benzaid, C.; Saiah, A.; Badache, N.; , "Secure pairwise broadcast time synchronization in wireless sensor networks," Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on , vol., no., pp.1-6, 27-29 June 2011 .

[18] Ortolani, S.; Conti, M.; Crispo, B.; Di Pietro, R.; , "Events privacy in WSNs: A new model and its application," World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a , vol., no., pp.1-9, 20-24 June 2011.

[19] K. Ren, W. Lou, and Y. Zhang, "LEDS: providing location-aware end-to-end data security in wireless sensor networks," IEEE Trans. MobileComput., vol. 7, no. 5, pp. 585-598, May 2008.

[20] S. Patil, "Sensor network traffic-adaptive key management scheme," in Proc. International Conf. Advances Recent Technol. Commun. Comput.,pp. 610-614, 2009.

[21] Y. Qian, K. Lu, B. Rong, and D. Tipper, "A design of optimal key management scheme for secure and survivable wireless sensor networks,"Security Commun. Netw., vol. 1, no. 1, pp. 75-85, 2008.

[22] C. Wang, T. Hong, G. Horng, and W. Wang, "A ga-based keymanagement scheme in hierarchical wireless sensor networks," International J. Innovative Comput., Inf. Control, 2008.

[23] G. Wang, G. Cao, and T. L. Porta, "Movement-assisted sensor deployment,"in Proc. IEEE Conf. Comput. Commun., Mar. 2004.

[24] S. Chellappan, W. Gu, X. Bai, B. Ma, D. Xuan, and K.Zhang, "Deploying wireless sensor networks under limited mobility constraints," IEEE Trans. Mobile Comput., vol. 6, no. 10, Oct. 2007.

[25] P. Andreou, D. Zeinalipour-Yazti, P. Chrysanthis, and G. Samaras, "Innetwork data acquisition and replication in mobile sensor networks,"Distributed Parallel Databases, pp. 1-26, 2011.

[26] C. Wang, P. Ramanathan, and K. Saluja, "Modeling latency-lifetime trade-off for target detection in mobile sensor networks," ACM Trans. Sensor Netw., vol. 7, no. 1, pp. 1-24, 2010.

[27] S. Choi, V. Sarangan, and S. Trost, "Key management in wireless sensor networks with inter-network sensor roaming," in 33rd IEEE Conf. Local Comput. Netw., 2008.

[28] Y. Lee and S. Lee, "A new efficient key management protocol for wireless sensor and actor networks," Arxiv preprint arXiv:0912.0580, 2009.

[29] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, "Group-based key management for mobile sensor networks," in Proc. IEEE Sarnoff Symp., pp. 1-5, 2010.

[30] Y. Lee and S. Lee, "A new efficient key management protocol for wireless sensor and actor networks," Arxiv preprint arXiv:0912.0580, 2009.

[31] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, "Group-based key management for mobile sensor networks," in Proc. IEEE Sarnoff Symp., pp. 1-5, 2010.

[32] A. Willig, "Wireless sensor networks: concept, challenges and approaches", Elektrotechnik &Informationstechnik, 2006.

[33] C. Cordeiro, D. Agrawal," AD HOC & SENSOR NETWORKS: Theory and Applications", book Published by World Scientific, 2006.

[34] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing 17:367-388, 2007. [2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam.

[35] Jianmin Zhang , Wenqi Yu and Xiande Liu ,"CRTBA: Chinese Remainder Theorem- Based Broadcast authentication in Wireless Sensor Networks,2009.

[36] Taekyoung Kwon and Jin Hong, "Secure and Efficient Broadcast Authentication in Wireless Sensor Networks," IEEE Transactions on computers, Vol.59, No.8,August 2010.

[37] Mark Hempstead, Michael J. Lyons, David Brooks, and Gu-Yeon Wei, "Survey of Hardware Systems for Wireless Sensor Networks,"Journal of Low Power Electronics Vol.4, 1–10, 2008.

[38] Elaine Shi and Adrian Perrig," Designing Secure Sensor Networks," IEEE Wireless Communications, December 2004.

[39] Mohsen Sharifi, Saeed Sedighian Kashi and Saeed Pourroostaei Arda-

kani,"LAP: A Lightweight Authentication Protocol for Smart Dust Wireless Sensor Networks",2008.