ISSN 2347-3487

Security in Wireless Sensor Networks

Barinder Paul Singh [1],Anish Arora[2] , Ashish Kumar [3]
Asst. prof. [1.2]
Ferozepur college of Engg. & Tech., Ferozepur
Asst proff., college fcet, ferozshah[3]
barinder.singh88@gmail.com1
anisharora87@gmail.com [2]
Kumar20.ashish@gmail.com[3]

Abstract:-Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

Keywords:-Sensor, Security, Attack, Holistic, Challenge.

Council for Innovative Research
Peer Review Research Publishing System
Journal: Journal of Advances In Physics
Vol 1, No 1
editor@cirworld.com
www.cirworld.com, member.cirworld.com

Introduction

A Wireless Sensor Network (WSN) distinguishes from other wireless or wired networks through its capability of interaction with the environment. Such networks have been proposed for various applications including search and rescue, disaster relief, smart environments, and localization systems. These applications require a large amount of battery-powered wireless sensors, and are generally designed for long-term deployments with no human intervention. Consequently, energy efficiency is one of the main design objectives for these sensor networks.

The main causes of the energy wastage are:

• **Collision:** occurs when two or more nodes attempt to transmit a packet across the network at the same time. The transmitted packets must be discarded and then retransmitted, thus the retransmission of those packets increases the energy consumption and the latency.

• **Overhearing**: occurs when a node receives a packet destined to other nodes. Overhearing

can be a major reason of energy waste mainly with a high node density causing a heavy traffic load.

• **Packet Overhead:** sending and receiving control packets consumes energy too and less

useful data packets can be transmitted, since control messages does not contain any useful

application data.

• **Idle listening:** it occurs when a sensor node listens to an idle channel to receive possible traffic. Usually a node in a WSN doesn't know when to wake up to receive a packet, thus it must keep its radio ON which consumes most of the energy. Therefore, researchers give a growing interest on optimizing WSN MAC (Medium Access Control) to reduce the energy consumption of the sensors in order to extend the network lifetime. The main challenge of any MAC protocol is to avoid collision as it represents the most important issue of energy saving. Usually in WSNs several nodes share the same channel, thereby the probability of packet collision increases. Developing a MAC protocol to coordinate the channel access of these nodes decreases the risk of packet collision and specially DATA packet collision which decreases the channel utilization as DATA packets are longer than control packets. In this paper, we provide a state-of-the-art study of WSN MAC protocols, and we will discuss the advantages as well as the drawbacks of the main existing solutions. We classify the MAC protocols according to the technique being used and to the problems they try to solve. In contrast to previous surveys, we will give more interest to the solutions treating the mobility of the sensor nodes and the real time constraints. Generally, MAC protocols are classified into two categories: contention based and schedule based protocols. Contention based protocols allow many users to use the same radio channel without pre-coordination. The main idea of these protocols is to listen the channel before sending the packet, IEEE 802.11, ALOHAandCSMA (Carrier Sense Multiple Access) are the most well known contention-based protocols. Compared to the schedule based protocols, the contention one are simple, because they don't require global synchronization, or topology knowledge which allows some nodes to join or to left the network few years after deployment. Message collisions, overhearing and idle listening are the main drawbacks of this approach.

Security Threats and Issues in Wireless Sensor Networks

Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided

than those of the guided transmission medium. he broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks. These issues are well-enumerated in some past researches [16], [17], [18] and also a number of security schemes are already been proposed to fight against them. However, the security mechanisms devised for wireless ad hoc networks could not be applied directly for wireless sensor networks because of the architectural disparity of the two networks. While ad hoc networks are self-organizing, dynamic topology, peer to peer networks formed by a collection of mobile nodes and the centralized entity is absent [19]; the wireless sensor networks

could have a command node or a base station (centralized entity, sometimes termed as sink). The architectural aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively in this case. Nevertheless, the major challenge is induced by the constraint of resources of the tiny sensors. In many cases, sensors are expected to be deployed arbitrarily in the enemy territory (especially in military reconnaissance scenario) or over dangerous or hazardous areas. Therefore,

even if the base station (sink) resides in the friendly or safe area, the sensor nodes need to be protected from being compromised.

Proposed Security Schemes and Related Work

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review and map various security schemes proposed or implemented so far for wireless sensor networks.

Security Schemes for Wireless Sensor Networks

[26] gives an analysis of secure routing in wireless sensor networks. [24] studies how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's life time. [7] aims at increasing energy efficiency for key management in wireless sensor networks and uses Younis et. al. [26] network model for its application. Wood et al. [21] studies DoS attacks against different layers of sensor protocol stack. JAM [28] presents a mapping protocol which detects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming.In [29] the authors show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks. Ye et. al. [23] presents a statistical en-route filtering (SEF) mechanism to detect injected false data in sensor network and focus mainly on how to filter false data using collective secret and thus preventing any single compromised

node from breaking the entire system. SNEP & µTESLA [6] are two secure building blocks for providing data confidentiality, data freshness and broadcast authentication. TinySec [25] proposes a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption protocol. Newsome et. al. [24] proposes some defense mechanisms against sybil attack in sensor networks. Kulkarni et al. [28] analyzes the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their communication and points out possible ways of sharing the secrets. [20] presents a probabilistic secret sharing protocol to defend Hello flood attacks. The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack.

Holistic Security in Wireless Sensor Networks

A holistic approach [27] aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option. Holistic view of Security in wireless sensor networks .The holistic approach has some basic principles like, in a

given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If

security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building ecurity layers as in the holistic approach, protection could be established for the overall network.

Conclusion

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

REFERENCES

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol.47, No. 6, June 2004, pp. 30-33.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.

[3] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[4] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[5] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., “Security for Sensor Networks”, CADIP Research Symposium, 2002,

[6] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., “SPINS: Security Protocols for Sensor Networks”, Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.

[7] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., “A Low-Energy Key Management Protocol for Wireless Sensor Networks”, Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.

[8] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M., and Tuan, T., “PicoRadios for wireless sensor networks: the next challenge in ultra-low power design”2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 – 201.

[9] Hollar, S, “COTS Dust”, Master’s Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.

[10] Saleh, M. and Khatib, I. A., “Throughput Analysis of WEP Security in Ad Hoc Sensor Networks”, Proc. The Second International Conference on Innovations in Information Technology (IIT’05), September 26-28, Dubai, 2005.

[11] Kurak, C and McHugh, J, “A Cautionary Note on Image Downgrading in Computer Security Applications”, Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp. 153-159.

[12] Mokowitz, I. S., Longdon, G. E., and Chang, L., “A New Paradigm Hidden in Steganography”, Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41 – 50.

[13] Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H-W., “Steganalysis on BPCS Steganography”, Pacific Rim Workshop on Digital Steganography (STEG’03), July 3-4, Japan , 2003.

[14] Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., “On handling QoS traffic in wireless sensor networks”, Proc. of the 37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004, pp. 292 – 301.

[15] Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., “Channel synthesized modulation employing singular vector for secured access on physical layer”, IEEE GLOBECOM 2003, Volume 3, 1-5 December, 2003, pp. 1226 – 1230

[16] Zhou, L. and Haas, Z. J., “Securing ad hoc networks”, IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30.

[17] Strulo, B., Farr, J., and Smith, A., “Securing Mobile Ad hoc Networks — A Motivational Approach”, BT Technology Journal, Volume 21, Issue 3, 2003, pp. 81 – 89.

[18] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications, Volume 11, Issue 1, February 2004, pp. 38 – 47.

[19] Pathan, A-S. K., Alam, M., Monowar, M., and Rabbi, F., “An Efficient Routing Protocol for Mobile Ad Hoc Networks with Neighbor Awareness and Multicasting”, Proc. IEEE E-Tech, Karachi, 31 July, 2004, pp. 97-100.

[20] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., “Analyzing interaction between distributed denial of service attacks and mitigation technologies”, Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[21] Wang, B-T. and Schulzrinne, H., “An IP traceback mechanism for reflective DoS attacks”, Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[22] Pfleeger, C. P. and Pfleeger, S. L., “Security in Computing”, 3rd edition, Prentice Hall 2003.

[23] Douceur, J. “The Sybil Attack”, 1st International Workshop on Peer-to-Peer Systems (2002).

[24] Newsome, J., Shi, E., Song, D, and Perrig, A, “The sybil attack in sensor networks: analysis & defenses”, Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[25] Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSR MANETs”, Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[26] Karlof, C. and Wagner, D., “Secure routing in wireless sensor networks: Attacks and countermeasures”, Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[27] Hu, Y.-C., Perrig, A., and Johnson, D.B., “Packet leashes: a defense against wormhole attacks in wireless networks”, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[28] Kulkarni, S. S., Gouda, M. G., and Arora, A., “Secret instantiation in adhoc networks,” Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.

[29] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., “A pairwise key pre-distribution scheme for wireless sensor networks”, Proc. of the 10th ACM conference on Computer and communications security, 2003, pp. 42-51