Volume 3, Issue 2, February 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Stochastic Analysis of Various Security Protocols in Wireless Sensor Networks

C. Anuradha
Assistant Professor
Department of Computer Science
Ramanujam Centre for Computational Intelligence
Bharath University,
Chennai,Tamilnadu,
India

Abstract— A wireless sensor network is a collection of nodes organized into a cooperative network, accommodate various sensors which communicate wirelessly. It is an emerging technology used in applications for mass public and military. As WSN uses inherent resource and computing constraints, it faces severe security challenges. In this paper, we discuss various security issues related with wireless sensor networks and how these issues are handled with various security mechanisms.

Index Terms— sensors, attacks, DoS, Nework layer

1. INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as a new technology in the IT ecosystem and a rich domain of active research involving hardware and system design, networking,distributed algorithms, programming models, data management, security and social factors .WSNs are being employed in various real time applications like Military, Disaster detection and relief, industry, Environmental Monitoring and Agriculture Farming etc. Due to the vast diversity of so many real time scenarios, security for WSNs becomes an important issue. For each implementation, there are different type of attacks possible and demands a different security mechanism.

The attractive features of the wireless sensor networks tempted many researchers to work on various issues related to this kind of networks. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are receiving extensive focus. In this paper, we explore the various security issues and challenges for next generation wireless sensor networks. Also it discusses the crucial parameters that require extensive investigations.

2. WSN ARCHITECTURE

In a typical WSN we see following network components –

- Sensor motes (Field devices) – Field devices are mounted in the process and they must be capable of routing packets on behalf of other devices. In most of the cases they characterize or control the process or process equipment. A router is a special type of field device which does not have process sensor or control equipment and it does not interface with the process itself.

- Gateway or Access points – A Gateway enables communication between Host application and field devices.

- Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

- Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

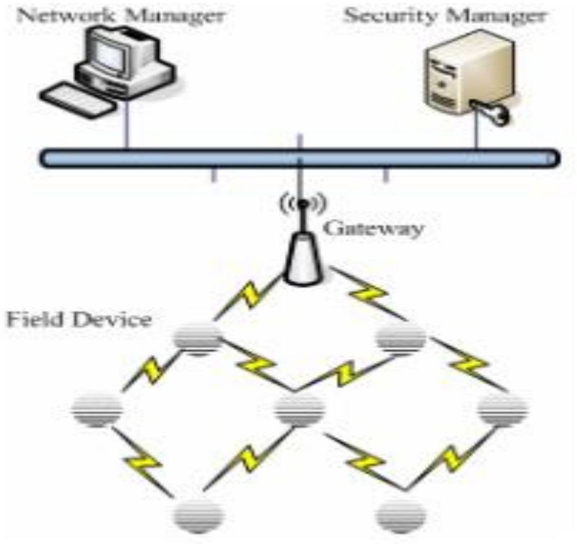


Figure 1 WSN Architecture

3. Obstacles of Sensor Security

A wireless sensor network is a special network that has many constraints compared to a traditional computer network. Because of these constraints it is difficult to directly employ the existing security approaches to the wireless sensor networks. Therefore, to develop useful security mechanisms
while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first .

3.1. Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a wireless sensor.

3.2. Limited Memory and Storage Space

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an efficient security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage . With such a limitation, the software built for the sensor must also be quite small. The total code space of TinyOS, the de-facto standard operating system for wireless sensors, is approximately 4K , and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

3.3 Power Limitation Energy

It is the biggest constraint to the capabilities of wireless sensor. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge should be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

4. Attacks in Wireless Sensor Networks

4.1. Denial of Service

Denial of Service (DoS) is any event that reduces or eliminates the capacity of a network to perform its expected function . The following are the different types of attacks under DoS.

1. DoS/Physical Layer/Jamming: Jamming. To jam a node or set of nodes, in this case, this is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network. Jamming the channel with an interrupting signal.

2. DoS/Physical Layer/Tampering. Physical Tampering. Nodes are vulnerable to physical harm, or tampering (i.e. reverse engineering).
3. DoS/Data Link Layer/Collision.
4. DoS/Data Link Layer/Exhaustion.
5. DoS/Data Link Layer/Unfairness.
6. DoS/Network Layer/Neglect and Greed.
7. DoS/Network Layer/Homing.
8. DoS/Network Layer/Spoofing. Misdirection. In this type of attack adversaries may
be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.
9. DoS/Network Layer/Black Holes.
10. DoS/Network Layer/Flooding.
11. DoS/Transport Layer/Flooding.
12 . DoS/Transport Layer/De-synchronization.

4.2. Sybil

Sybil attack is defined as a malicious device illegitimately taking on multiple identities. Using this type of attack , a single node presents multiple identities to other nodes in the network which can be used to significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, dispersity and multipath. It is extremely difficult to launch such an attack in a network because every pair of neighboring nodes uses a unique key to initialize frequency hopping.Sybil attack also poses a significant threat to geographic routing protocols.

.

4.3. Wormhole

In this kind of attack, an adversary tunnels messages received in one part of the network over a low latency link and it replays them in a different part. An adversary which is situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary can convince nodes who would normally be multiple hops from a base station that they are only few or two hops away via the wormhole. This will create a sinkhole because the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station. Potentially all traffic in the surrounding area will be drawn through it if alternate routes seem to be significantly less attractive.

4.4. Sinkhole (Black hole)

Sinkhole attacks work by making a compromised node look and it is especially attractive to surrounding nodes with respect to the routing algorithm and nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks could enable many other attacks (eg. selective forwarding).

4.5. Selective Forwarding

In a selective forwarding attack, malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any
further. However, such an attacker runs the risks that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing.

4.6. Hello Flood

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor and begin changing information with the nodes.

5. Defensive Measures

Now we are in a position to describe the measures for satisfying security requirements, and protecting the sensor network from attacks. We start with key establishment in wireless sensor networks, which lays the foundation for the security in a wireless sensor network, followed by defending against DoS attacks, secure broadcasting and multicasting, defending against attacks on routing protocols, combating traffic analysis attacks, defending against attacks on sensor privacy, intrusion detection, secure data aggregation, defending against physical attacks, and trust management.

5.1. Security Schemes for Wireless Sensor Networks

Studies revealed 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. It aims at increasing energy efficiency for key management in wireless sensor networks and uses Younis et. al. network model for its application. Wood et al. studies DoS attacks against different layers of sensor protocol stack. JAM presents a mapping protocol which etects 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 another study, 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. 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 are two secure building blocks for providing data confidentiality, data freshness and broadcast authentication. TinySec proposes a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption protocol.

Newsome et. al. proposes some defense mechanisms against sybil attack in sensor networks. Kulkarni et al. 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. In another paper, a probabilistic secret sharing Protocol has been defined 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.

5.2. Holistic Security in Wireless Sensor Networks

A holistic approach 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 allthe 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.

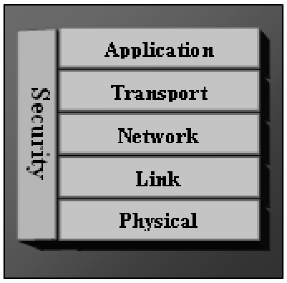


Figure 2: Holistic view of Security in wireless sensor networks

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 security layers as in the holistic approach, protection could be established for the overall network.

5.3. Host Based Security

We should be concentrating more on sensor node themselves, because nearly all attacks on WSN starts from compromising a node. Since physical tampering can not be avoided. Care must be taken to prevent software based tempering. There are enough chances that applications/operating system running in sensor node are vulnerable to popular exploits such as buffer overflow.Here, the problem is with composing the components of the overall system. A secure system can be realized only by building security into the system architecture and this requires

1) Security analysis of the architecture.
2) Security testing of the realized system for implementation bugs.
3) Removal/scrutiny of "undocumented features" that can be potentially exploited to violate the system security.

5.4. Network Based Security

Network based security can be mainly characterized as

1) Security for fundamental Services: - There are some fundamental operations like clustering or group management and data aggregation which require attention. So we choose a game theoretic model for that purpose, here the game is defined in between sensor nodes and more a sensor node cooperates, better will be its reputation. ISA for a node will store reputation factor for all neighbouring nodes and depending on the reputation it will forward a packet to that node. A very good approach using game theory is given in [9] ,which defines a payoff utility function, according the value of payoff utility function, clustering can be done. ISA will maintain a small history table which helps the node in making strategy, if the node to which it wants to communicate has enough reputation level and good history of joint operation, then the strategy will be to cooperate else to oppose. There is an open research challenge to define a strategy set which can formulate a non cooperative strategy between an intruder and a sensor node. If cluster formed is secure, then data aggregation will also be secured

2) Cryptography: - It has been shown by recent works in security that strong cryptography can be equated with strong security or even usable security is a myth [5]– while strong cryptography may be necessary, it definitely is not sufficient to realize a system with the required security properties. So we should use cryptography, but without ignoring security of fundamental components. WSN also requires various authentication and encryption mechanisms but of different level. Consider following examples:-

1. A routing packet and aggregated data packet containing confidential information can not be encrypted by same level of cryptography.

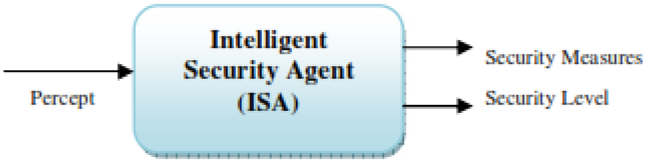
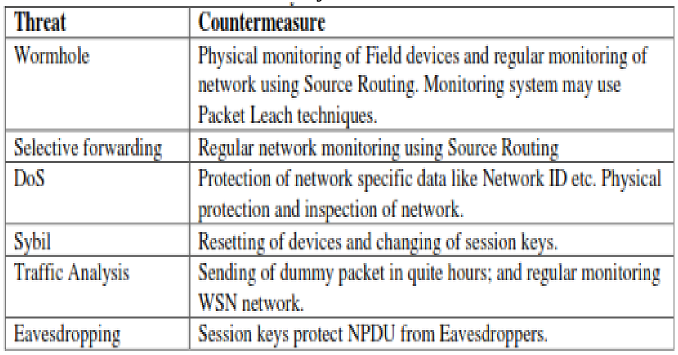


Fig 3.ISA for cryptographic means

2. Suppose one sensor network is deployed in Military Surveillance System and other in agricultural faming, so in both the network encryption level should be different based on risks and efficiency.

Here the function of ISA comes, depending on current percept it will determine an adaptive reaction for level of security that would incorporate many policies and recommendations can also be given at deployment or afterwards.

Table 1: Network layer threats and measures



Threat	Countermeasure
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use Packet Leach techniques.
Selective forwarding	Regular network monitoring using Source Routing
DoS	Protection of network specific data like Network ID etc. Physical protection and inspection of network.
Sybil	Resetting of devices and changing of session keys.
Traffic Analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network.
Eavesdropping	Session keys protect NPDU from Eavesdroppers.

6. Conclusion

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a fool proof security to the network. In this paper, we have made a threat analysis to the Wireless Sensor Network and suggested some counter measures. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

REFERENCES

[1] Yee Wei Law Paul J.M. Havinga,"How to Secure a Wireless Sensor Network", ISSNIP 2005,IEEE 2005, pp(89-95).

[2] Al-Sakib Khan Pathan et . al. "Security in Wireless Sensor Networks: Issues and Challenges" in Feb. 20-22, 2006, ICACT2006, ISBN 89-5519129-4pp(1043-1048).

[3] Mingbo Xiao, Xudong Wang, Guangsong Yang,"Cross-Layer Design for the Security of Wireless Sensor Networks", Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21 - 23, 2006, Dalian, China, pp(104-108).

[4] M Healy, T Newe and E Lewis,"Resources Implications for Data Security in Wireless Sensor Network Nodes" in Sensor Comm 2007,pp(170-175).

[5] Sanjay Burman,"Cryptography & Security - Future Challenges and Issues",Invited Talk, in proc. of ADCOM 2007.

[6] Dr. Sami S. Al-Wakeel and Eng. Saad A. AL-Swailem,"PRSA: A Path 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] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review, vol. 4, no. 5, October 2001.

[12] A. Perrig, R. Szewczyk, V.Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of Mobile Networking and Computing 2001, 2001.

[13] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, vol. 8, no. 2-3, pp. 169-185, 2002.

[14] M.-J. Lin, K. Marzullo, and S. Masini, "Gossip versus deterministic flooding: Low message overhead and high reliability for broadcasting on small networks, Tech. Rep. CS1999-0637, 18, 1999.

[15] L. Li, J. Halpern, and Z. Haas, "Gossip-based ad hoc routing," in IEEE Infocom 2002, 2002.

[16] Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.