ENHANCEMENT OF SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORK

KRISHNA VEER SINGH
Assistant Professor
IIMT College of Engineering
Greater Noida

KAMLESH KUMAR PATHAK
Assistant Professor
IIMT College of Engineering
Greater Noida

ABSTRACT: Wireless Sensor Networks (WSNs) are a new technology foreseen to be used increasingly in the near future due to their data acquisition and data processing abilities. Security for WSNs is an area that needs to be considered in order to protect the functionality of these networks, the data they convey and the location of their members. The security models & protocols used in wired and other networks are not suited to WSNs because of their severe resource constrictions.

In this paper highlight the research in the area of security for WSNs and propose a solution based on intrusion detection systems and efficient classifiers. My hope is to generate a security model that will provide energy efficiency and fault tolerance to WSNs under attack.

KEYWORDS: Wireless Sensor Network (WSN), Security

I. INTRODUCTION

Wireless Sensor Networks (WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention.

The individual nodes that constitute a wireless sensor network are generally small in size and use power-efficient batteries to extend their operational longevity. Depending on its function, each node has a sensor board that facilitates the detection and measurement of heat, vibrations, air-pressure and magnetic fields**.** Advancements in Micro Electro Mechanical Systems (MEMS) and wireless networks have made possible the advent of tiny sensor nodes sometimes referred as “motes”. *Motes* developed at UC Berkeley and manufactured by Crossbow. These are mini, low-cost devices with limited coverage having low power, smaller memory sizes and low bandwidth. Motes make use of Tiny OS, an operating system designed from scratch to be as power-efficient as possible.

Security Framework WSNSF (Wireless Sensor Networks Security Framework) to provide a comprehensive security solution against the known attacks in sensor networks. The proposed framework consists of four interacting components: a secure triple-key (STKS) scheme, secure routing algorithms (SRAs), a secure localization technique (SLT) and a malicious node detection mechanism.

Security framework that adheres to the four security goals: Confidentiality, Integrity, Authentication and Availability through a secure key scheme, secure routing algorithms, secure localisation and a monitoring mechanism to detect malicious nodes in the network.

In order to develop and evaluate the performance of a new solution for wireless sensor networks in terms of energy and memory consumption The comparative analysis focused on a well known link layer security protocol TinySec [Karlof et al., 2004].

The proposed security framework is aimed at overcoming the weaknesses of existing solutions by recognising the node limitations and compensating for these, based on the belief that security in sensor networks is all about mitigating the attacks.

II. SECURITY ANALYSIS

A sensor network should not leak sensor readings to neighbouring networks. In many applications (e.g., key distribution) nodes communicate highly sensitive data. Set up secure channels between nodes and base stations and later bootstrap other secure channels as necessary. Data authentication allows a receiver to verify that the data really was sent by the claimed sender. In communication, data integrity ensures the receiver that the received data is not altered in transit by an adversary. Sensor networks send measurements over time, so it is not enough to guarantee confidentiality and authentication, must ensure each message is fresh.

A. DESIGN GOALS

Confidentiality: To prevent malicious nodes from claiming a different legitimate –seeming location in the network, the source should only help the sensor node in determining its location. Neither the source's location nor the node's location should be disclosed at any point.

Integrity: Information coming from the source should be ascertained as unaltered and trustworthy before a sensor node uses it to discover its location.

Availability: The information required to compute the location of the sensor node should be available whenever needed.

Non-repudiation: Neither the source provides the information nor the sensor node requesting it should be able to deny the information exchange.

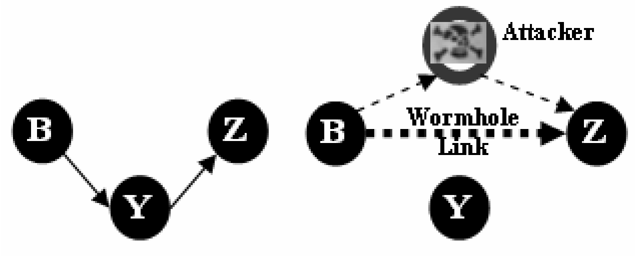
- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

1. WSN SECURITY FRAMEWORK

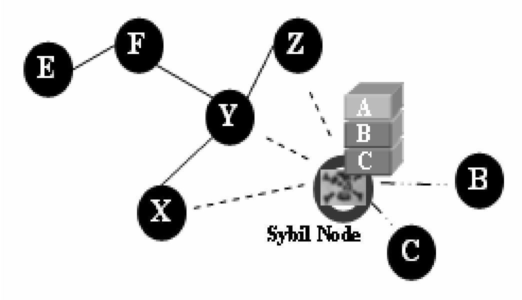
Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories:

1. Spoofed, altered, or replayed routing information
2. Selective forwarding
3. Sinkhole attacks
4. Sybil attacks
5. Wormholes
6. HELLO flood attacks
7. Acknowledgement spoofing

ATTACKS	DESCRIPTION
Spoofed, altered, or replayed routing Information	Create routing loop, attract or repel network traffic, extend or shorten source routes, generate false error messages etc
Selective forwarding	Either in-path or beneath-path by deliberate jamming controls which information is forwarded. A malicious node acts like a black hole and refuses to forward every packet it receives.
Sinkhole attacks	Attracting traffic to a specific node, e.g. to prepare selective forwarding.
Sybil attacks	A single node presents multiple identities, allows to reduce the effectiveness of fault tolerant schemes such as distributed storage and multi-paths etc.
Wormhole attacks	Tunnelling of messages over alternative low-latency links to confuse the routing protocol, creating sinkholes etc.
HELLO floods	An attacker sends or replays a routing protocol's HELLO packets with more energy.



Wormhole attack



Sybil Attack

B. LAYERING-BASED SECURITY APPROACH

	Attack types	Countermeasures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Network Layer	Wormholes, Sinkholes, Sybil Attacks, Routing Loops	Key Management, Secure Routing
Data Link Layer	Link Layer Jamming	Link Layer Encryption
Physical Layer	DoS and Node capture attacks	Adaptive antennas, Spread Spectrum

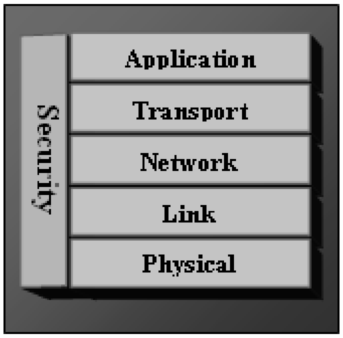
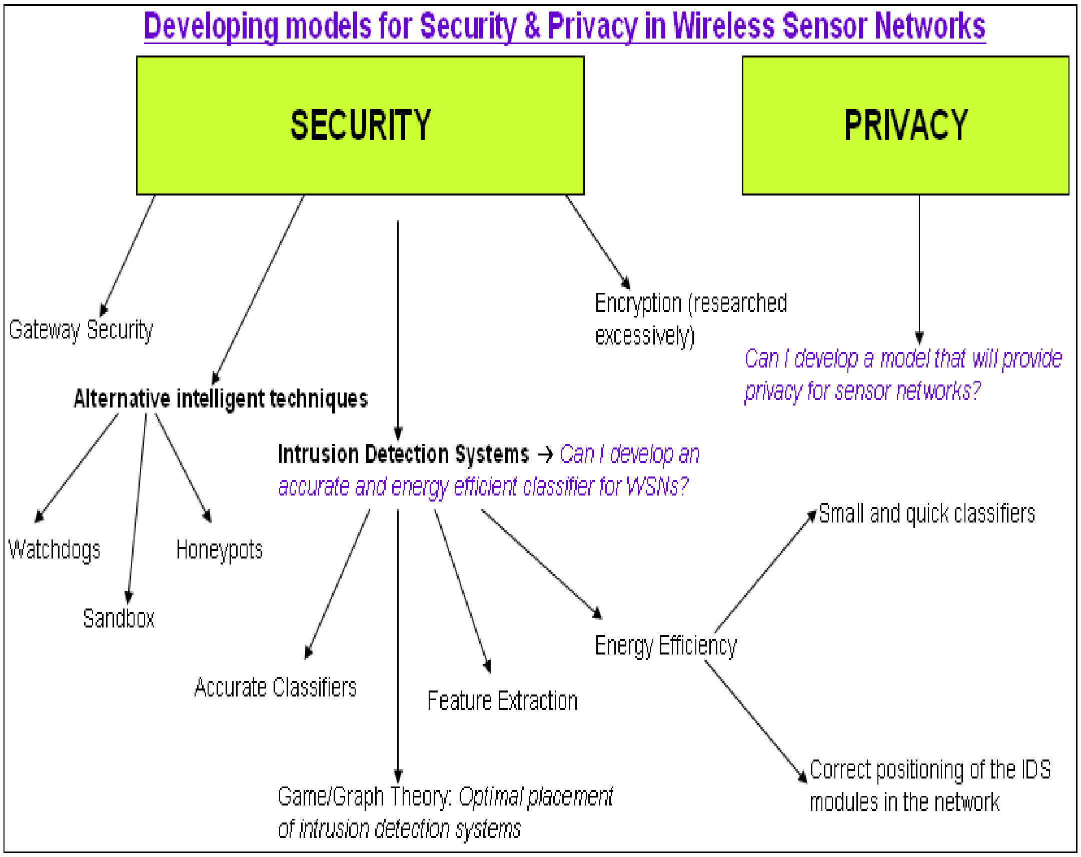


Fig: Holistic view of Security in wireless sensor networks

C. SUMMARY OF ATTACKS AGAINST SENSOR NETWORK ROUTING PROTOCOLS

Protocol	Relevant attacks
Tiny OS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil attacks, wormholes, HELLO floods
Directed Diffusion and its multi-path variant	Bogus routing information, selective forwarding, sinkholes, Sybil attacks, wormholes, HELLO floods
Geographic Routing (GPSR,GEAR)	Bogus routing information, selective forwarding, Sybil attacks
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering-based protocols (LEACH, TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil attacks, wormholes
Energy conserving topology Maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

2. SECURITY & PRIVACY IN WSN


Developing models for Security & Privacy in Wireless Sensor Networks
SECURITY
PRIVACY
Gateway Security
Alternative intelligent techniques
Encryption (researched excessively)
Can I develop a model that will provide privacy for sensor networks?
Intrusion Detection Systems → Can I develop an accurate and energy efficient classifier for WSNs?
Watchdogs
Honeypots
Sandbox
Small and quick classifiers
Energy Efficiency
Accurate Classifiers
Feature Extraction
Game/Graph Theory: Optimal placement of intrusion detection systems
Correct positioning of the IDS modules in the network

III. CONCLUSIONS

Wireless sensor networks are a unique class of mobile ad hoc network consisting of tiny low-cost resource constrained devices that have the ability to sense their environment, to in process, to aggregate and to send the data to a destination. The deployment nature and limitations of the nodes resources as well as the wireless communication channel make sensor networks susceptible to a variety of new attacks in addition to the attacks which occur in mobile ad hoc networks. Deployment of sensor networks has been envisioned in many sensitive applications such as military operations and health care. Despite advances in miniaturization and other developments in sensor networks occurring at a very fast pace, security within sensor networks has not gained significant interest. This is partially because of the lack of understanding of the potential of these tiny devices, and partially due to the lack of commercial motivation. So far, there has been no single application for sensor networks which has been able to attract commercial public interests. Traditional security measures require heavy communication and computational resources which are beyond the resource starved sensor nodes. In this research, it has been argued that cryptographically complex security solutions for sensor networks are not viable for many reasons: firstly, the energy, memory and transmission range limitations; secondly, the wireless channel limitations; thirdly, the deployment nature of sensor nodes being left unattended after deployment; and fourthly, the need to keep costs low to enable dense deployment. Instead, sensor networks need a balanced and comprehensive solution, which is efficient, effective and has low security overheads. Bearing these factors in mind, a novel security framework for wireless sensor networks has been proposed.

REFERENCES

1. Akkaya, K. and Younis, M. (2003) A survey on routing protocols for wireless sensor networks. Elsevier Journal of Ad Hoc Netwoks, 3, pp. 325-349.
2. Akyildiz, I.F., Su, W., Sankarasubramaniam Y. and Cayirci, E. (2002) Wireless sensor networks: A survey. Computer Networks, 38 (4) March, pp. 393-422.
3. A Security framework for wireless sensor networks Tanveer Ahmad Zia February 2008Al-Karaki, J. and Kamal, A. (2003) Routing techniques in wireless sensor networks: A survey. Lowa, USA, Lowa State University.
4. Hu, N., Smith R.R.K. and Bradford, P.G. (2004) Security for fixed sensor networks. In Proceedings of the 42nd Annual Southeast Regional Conference, April 2- 3, 2004. Huntsville, Alabama, USA, ACM Press.
5. Hu, F., Ziobro, J., Tillett, J. and Sharma, N. (2004) Secure wireless sensor networks: Problems and Solutions. Journal on Systemic, Cybernetics and Informatics, 1 (9).
6. Karlof, C. and Wagner, D. (2003) Secure routing in wireless sensor networks: attacks and countermeasures. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1 (2-3), pp. 293-315.
7. Karlof, C., Shastry, N. and Wagner, D. (2004) Tinysec: link layer security architecture for wireless sensor networks. In Proceedings of SenSys'04, November 3-5, 2004, Baltimore, Maryland, USA.
8. Perrig, A., Szewczyk, R., and Wen, V., Culler, D. and Tygar, J.D. (2002) SPINS: security protocols for sensor networks. In Wireless Networks Journal (WINE), September 2002.
9. Perrig, A., Stankovic, J. and Wagner, D. (2004) Security in wireless sensor network. Communication of the ACM, 47 (6).
10. Wireless sensor networks: a survey I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci Received 12 December 2001; accepted 20 December 2001
11. Security in Wireless Sensor Networks: Issues and Challenges Al-Sakib Khan Pathan Department of Computer Engg. Kyung Hee University, Korea spathan@networking.khu.ac.kr Hyung-Woo Lee Department of Software Hanshin University, Korea hwlee@hs.ac.kr Choong Seon Hong Department of Computer Engg. Kyung Hee University, Korea cshong@khu.ac.kr