A Survey on Security Frameworks for Cluster Based Wireless Sensor Networks

Shital Mane[1], Madhav Ingle[2]

[1]M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India.
Savitribai Phule Pune University, Pune, Maharashtra, India -411028

[2]M.E coordinator and Assistant Professor, (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411028

Abstract: ***A wireless sensor network (WSN) is a network system for geographically distributed resources using wireless sensor nodes to observe physical or environmental conditions such as temperature, motion, and sound. The nodes are individually capable to send data to one or more collection points in a WSN to sense their environments and processing the information data locally. WSNs are great solutions for most applications and security is often a major concern. Though research regarding cryptography, secures routing, key management, intrusion detection, and secure data aggregation in WSNs is done until today, there are still some challenges to be addressed. These challenges are like first selection of proper cryptographic method second factors affecting sensors like memory, speed, and bandwidth, third challenge is, most of the available protocols assume that the sensor nodes and the base station are stationary. Sensor node and base stations in some situations like battlefield need to be mobile. The sensor network topology is been extensively affected by mobility of sensor nodes and so raises many issues about secure routing protocols. This paper surveys various security issues related to cluster based WSNs and existing security protocols.***

Keywords: Cluster-based WSNs, ID based digital signature, Secure data transmission, wireless sensor networks, secure routing protocol.

1. Introduction

Wireless Sensor Networks (WSNs) indicates massive improvement on traditional wired sensor networks. WSNs can greatly simplify system operation and design, as the environment being observed does not need the energy or communication infrastructure associated with wired networks [1]. WSNs are solving many applications like tracking and detecting the passage of tanks and troops on a battlefield, observing environmental pollutants, tracking the location of personnel in a building, and measuring traffic flows on roads. Mostly sensor networks posse's mission-critical tasks [2, 3] so security needs to consider. Using forged information or improper use of information results in unwanted information leakage and inaccurate results. As WSNs used more frequently and grow rapidly, the need for security in them becomes more obvious. However, the behavior of nodes in WSNs gives rise to limitations such as limited energy, processing capability, and storage capacity. These limitations make WSNs very distinct from traditional ad hoc wireless networks. As such, special techniques and protocols have discovered for use in WSNs.

A. Structure of WSNs

A WSN is generally collection of hundreds or thousands of sensor nodes. These sensor nodes are heavily arranged in a sensor field and have the ability to gather data and route data back to a base station (BS). A sensor has four basic parts: a processing unit, a transceiver unit, a power unit and a sensing unit [4]. It may also have extra application-dependent parts such as a power generator, mobilize, and location finding system. Sensing units is a collection of two subunits: analog-to-digital converters (ADCs) and sensors. The ADCs transfer the analog signals generated by the sensors to digital signals based on the observed circumstance. The processing unit, which is usually collide with a small storage unit, arrange the procedures that make the sensor node interact with the other nodes. A transceiver unit links the node to the network. One of the major units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells). Most of the sensor network sensing tasks and routing techniques require knowledge of location, which is been given by a location finding system. Lastly, a mobilize may sometimes be needed to move the sensor node, depending on the application. The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows [4]:

B. Attacks on each layer table

Layer	Responsible for	Attacks
Physical layer	Frequency selection, carrier frequency generation, signals deflection, modulation, and data encryption.	Jamming, Tampering
Data link layer	The multiplexing of data streams, data frame detection, medium access, and error control; as well as ensuring reliable point-to-point and point-to-multipoint connections.	Collisions, Exhaustion, Unfairness
Network layer	The assignment of addresses and how packets are forwarded	Spoofed, Altered, or Replayed Routing Information, Selective Forwarding, Sinkhole, Sybil, Wormholes, Hello Flood Attacks, Acknowledgment Spoofing
Transport layer	Specifying how the reliable transport of packets will take place	Flooding, Desynchronization
Application layer	Specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user.	

C. Constraints for WSNs

WSNs must consider the hardware constraints of the sensor nodes:

a) Energy: energy consumption in sensor nodes can be categorized into three parts:
  - Energy for the sensor transducer
  - Energy for communication among sensor nodes
  - Energy for microprocessor computation
  - Communication is more costly than computation in WSNs. Any message growth caused by security mechanisms comes at a great cost. Moreover, higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions. Thus, WSNs can be divided into different security levels, depending on energy cost.

b) Computation: the embedded processors in sensor nodes are generally not as powerful as those in nodes of a wired or ad hoc network. As such, complex cryptographic algorithms cannot be used in WSNs.

c) Memory: memory in a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate computations. There is usually not enough space to run complicated algorithms after loading OS and application code. In the SmartDust project, for example, TinyOS consumes about 3500 bytes of instruction memory, leaving only 4500 bytes for security and applications. This makes it impractical to use the majority of current security algorithms. With an Intel Mote, the situation is been slightly improved, but still far from meeting the requirements of many algorithms.

d) Transmission range: the communication range of sensor nodes is limited both technically and by the need to conserve energy. The actual range achieved from a given transmission signal strength is dependent on various environmental factors such as weather and terrain

D. Attacks in sensor networks can be classified into the following categories:

- *Outsider versus insider attacks*: outside attacks are defined as attacks from nodes, which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.
- *Passive versus active attacks*: passive attacks include eavesdropping on or monitoring packets exchanged within a WSN; active attacks involve some modifications of the data steam or the creation of a false stream.
- *Mote-class versus laptop-class attacks*: in mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes; in laptop-class attacks, an adversary can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes.

E. Currently wireless sensor network facing challenges like:

First, the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application-specific.

Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints.

Third, most of the current protocols assume that the sensor nodes and the base station are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile. The mobility of sensor nodes has a great influence on sensor network topology and thus raises many issues about secure routing protocols.

F. Issues in WSNs need to address:

Exploit the availability of private key operations on sensor nodes:

- Recent studies on public key cryptography show that public key operations may be practical in sensor nodes. However, private key operations are still too expensive to accomplish in a sensor node. As public key cryptography can greatly ease the design of security in WSNs, improving the efficiency of private key operations on sensor nodes is highly desirable.
- Secure routing protocols for mobile sensor networks:
  The mobility of sensor nodes has a great influence on sensor network topology and thus on the routing protocols. Mobility can be at the base station, sensor nodes, or both. Current protocols assume the sensor network is stationary. New secure routing protocols for mobile sensor networks need to be developed.
- Continuous stream security in WSNs:
  Current work on security in sensor networks focuses on discrete events such as temperature and humidity. Continuous stream events such as video and images are

not discussed. Video and image sensors for WSNs might not be widely available now, but will likely be in the future. Substantial differences in authentication and encryption exist between discrete events and continuous events, indicating that there will be distinctions between continuous stream security and the current protocols in WSNs.

- QoS and security:
  Performance is generally degraded with the addition of security services in WSNs. Current studies on security in WSNs focus on individual topics such as key management, secure routing, secure data aggregation, and intrusion detection. QoS and security services need to be evaluated together in WSNs.

2. Related Work

Wireless sensor networks are great solution for this communicated world by internet. Due to WSNs, it is possible that all the remote applications could come in our range [1, 3,4].However, this technology from its invention is still not overcome the issue of security which is challenge for researchers yet [2]. Although there are security protocols available to limit data, leakage there is still need to find proper solution. There are some existing protocols are mentioned in this survey as below.

1) LEACH Protocol[5]

In 2002, research [5] proposed an application specific protocol for wireless micro sensor network. In this research author developed and analyzed low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for microsensor networks that collects the concept of media access and energy-efficient cluster-based routing together with application-specific data aggregation to gain good performance in terms of system latency, application-perceived quality and lifetime. In this method LEACH algorithm adopt clusters and rotate cluster head to evenly distribute load among nodes. Results show that LEACH can improve system lifetime by an order of magnitude compared with general-purpose multihop approaches. Though this protocol is promising it is still need attention to make it perfect.

Constraints that limit applicability of LEACH are: In LEACH there is not efficient use of a bandwidth when not all nodes are been connected to cluster head due to sensors always transmit data to the cluster head during their allocated TDMA slot. Second, current design of a LEACH is not suitable for wider range of a micro sensor networks which limits scalability because here author assumed that all nodes are within communication range of each other and the base station. Third, using fixed clusters and rotating cluster head nodes within the cluster may require more transmit power from the nodes. Fourth here author showed that using data aggregation reduces energy dissipation and latency in data transfer compared with an approach like MTE that cannot take advantage of local data correlation.

2) Identity Based Security for Vehicular Ad-HOC Networks.[6]

Jinyuan Sun,et al. in 2010 [6] proposed a security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, nonrepudiation, message integrity, and confidentiality. Author contributed privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication.

Author contributions are: This is a pseudonym-based scheme to assure vehicle user privacy and traceability. Second, this design is a threshold signature-based scheme to achieve nonframeability in tracing law violators. In this scheme, an innocent vehicle could not framed by a corrupted law enforcement authority due to this role-splitting mechanism. Third, A novel privacy-preserving defense scheme is proposed leveraging threshold authentication. It guarantees that any additional authentication beyond the threshold will result in the revocation of the misbehaving users. Fourth, this scheme incorporates mechanisms that guarantee authentication, nonrepudiation, message integrity, and confidentiality.

However, this system achieves the predefined security objectives and desirable efficiencies it is not suitable for real time VANET settings.

3) Authentication Framework Based On Identity Based Signature For WSNs.[7]

To address the problem of authentication in WSNs, author proposed an efficient and secure framework for authenticated broadcast/multicast by sensor nodes as well as for outside user authentication, which utilizes identity based cryptography and online/offline signature schemes. The primary goals of this framework are to enable all sensor nodes in the network, firstly, to broadcast and/or multicast an authenticated message quickly; secondly, to verify the broadcast/multicast message sender and the message contents; and finally, to verify the legitimacy of an outside user. The proposed framework is been also evaluated using the most efficient and secure identity-based signature schemes. Existing broadcast authentication schemes in WSNs do not handle the problem of authenticated broadcast by sensor nodes proposed framework is efficient solution to this problem.

In future there is improvement to focus on user access control to provide a complete ID-based authentication framework which would enable the sensor nodes, on one hand, to broadcast a message to quickly respond to some critical situations and, on the other hand, to control user access according to his access privilege. In future proposed framework will upgrade on real sensor nodes to get actual results.

4) Secure Routing Protocol for Cluster-Based Wireless Networks [8].

In this approach, author introduced a novel secure routing protocol for cluster-based WSNs using ID-based digital signature. The proposed protocol is efficient in communication, and it achieves all the requirements in security for routing protocols in cluster-based WSNs. This scheme is been pointing the deficiency of the secure routing protocols with symmetric key pairing. However, the simulation results point out the issues in the proposed protocol that, the extra energy consumption by computation of the auxiliary security overhead is still large in the proposed protocol. The future work is to improve our simulation experiments with other secure routing protocols for better results, and improve the protocol in energy efficiency with pairing.

5) SET-IBS and SET-IBOOS protocols for Cluster Based Wireless Networks [9].

In this approach author combines features of two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme. Both the proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for CWSNs with concrete ID-based settings, which use ID information and digital signature for authentication. Thus, both SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs. Results show that the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

3. Conclusion

In this survey, our purpose is to review some existing security protocols in context of wireless sensor networks. Our motive was to study author's contributions and their advantages and limitations. According to authors, contributions this survey predicts that SET_IBS and SET_IBOOS are the efficient protocols until now for cluster based wireless networks to fulfill security requirements we can adopt this protocols in our design to fulfill goals of security in cluster based wireless sensor networks.

References

[1] D. Estrin *et al.*, "Instrumenting the World with Wireless Sensor Networks," *Proc. Int'l. Conf. Acoustics, Speech and Signal Processing*, Salt Lake City, UT, May 2001.

[2] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks", *IEEE Comp. Mag.*, Oct. 2003, pp. 103–05.

[3] E. Shi and A. Perrig, "Designing Secure Sensor Networks," *Wireless Commun. Mag.,* vol. 11, no. 6, Dec. 2004 pp. 38–43.

[4] I. F. Akyildiz *et al.*, "A Survey on Sensor Setworks," *IEEE Commun. Mag.*, vol. 40, no. 8, Aug. 2002, pp. 102–114.

[5] Wendi B. Heinzelman, Anantha P. Chandrakasan , Hari Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE Transactions On Wireless Communications, Vol. 1, No. 4, October 2002, pp. 660-670.

[6] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 21, No. 9, September 2010, pp. 1227-1239.

[7] Rehana Yasmin, Eike Ritter, Guilin Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures", IEEE International Conference on Computer and Information Technology, 2010, pp. 882-889.

[8] Huang Lu, Jie Li, and Hisao Kameda, "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature", IEEE Globecom 2010 proceedings, pp.1-4.

[9] Huang Lu, Jie Li, Mohsen Guizani, " Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 3, March 2014, pp. 750 761.

Author Profile

Ms. Shital Mane, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411028. She received her B.E (Computer) Degree from BIGCE, Solapur India. Solapur University , Solapur Maharashtra, India -411007. Her area of interest is Network Security and Data Mining.

Asst Prof. M.D Ingle, received his M Tech. (Computer) Degree from Dr. Babasaheb Ambedkar Technological University, Lonere, Dist. Raigad-402 103, Maharashtra, India. He received his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India.He is currently working as M.E coordinator and Asst Prof (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India - 411028. His area of interest is network security and Cloud Computing.