Securing Distributed Wireless sensor Networks: Issues and Guidelines

Riaz A. Shaikh, Young Jae Song, Sungyoung Lee
Computer Eng. Department, Kyung Hee University, Korea
Corresponding Author's Email Address: riaz@oslab.khu.ac.kr

ABSTRACT

With the emergence of ubiquitous computing the role of sensor network is becoming more important which demands highest level security and energy efficiency. In this paper we have investigated the current available solutions and found that none of the solutions are completely meeting the basic security requirements such as authentication, access control, and non-repudiation, etc. Therefore we have proposed "Tetra security Framework for the distributed wireless sensor networks" in order to achieve highest level security and overall energy efficiency.

1. INTRODUCTION

Sensor network is an emerging technology that will play a key role in sensing, gathering and propagating information about environmental phenomena. It consists of large number of small tiny sized sensor nodes, which are densely deployed in the environment [1]. The primary mission of sensor network is to detect and report events occurring with in the range of sensor network. Events can be any thing like movements of troops, movements of armed vehicles, detection of chemical occurrences etc. Once an event is detected, detecting sensor node may report the event directly to the remote command and control application or collaborate with other sensors in the network to more reliably identify and track a target. Sensor networks can be used for various application areas (e.g. health, military, home, etc). For different application areas there are different technical issues where researchers are currently working on.

Sensor Networks are based on wireless networks therefore they are more vulnerable from a security perspective as compared to wired networks. Much work has been done so far for providing security in a wireless networks, but unfortunately we can not use those solutions in wireless sensor networks because it has different characteristics. The basic difference between ad hoc wireless networks and sensor networks are [2]

- Sensor network's topology changes very frequently.
- Sensor nodes communicate with each other in a broadcast manner, whereas most nodes in ad hoc networks communicate with each other in a point-to-point manner.
- Power, computational capacities and memory are limited in sensor nodes.
- In a typical sensor network the numbers of nodes are much more than ad hoc networks.
- Due to large number of sensor nodes that are densely deployed in a sensor network may not have global identification (ID).

With the emergence of ubiquitous computing the role of sensor network is becoming more important and the need of security in ubiquitous sensor network environment is critical. There are two major constraints with wireless sensor networks which are making harder to implement security services.

1. Limited Memory and Storage Space: Commonly sensor nodes have 8-bit, 4 MHz CPU with only 8K (total) of memory and disk space.
2. Power Limitation: Another major constraint with wireless sensor is that of limited power. Before going to implement security functionalities (e.g. encryption, decryption, verifying data, signatures, key exchanges, etc), we need to take care of how much power would be consumed.

The objective of this work is to investigate the current state of the art security solutions that are specially developed for wireless sensor networks and find out their pros and cons. From investigation we found that none of the solutions provide complete security to the wireless sensor networks and most of them are providing security based on the assumption that the environment is trusted [3]. Therefore we have proposed our own "Tetra security Framework for the wireless sensor networks" in order to achieve highest level security and overall energy efficiency. The objective of Tetra security framework is to focus on solving many open questions [4] which are

- How much and what type of security is really needed?
- How can misbehave nodes be prevented from providing false data?
- How can we create the dynamic trust relationship among sensor nodes?
- Can energy and security be traded-off such that the level of network security can be easily adapted?

The rest of this paper is organized as follows: Section 2 discuses the security threads to distributed wireless sensor networks. Section 3 describes the basic security requirements. In section 4 we have given the comparison of existing security protocols. Section 5 describes proposed Tetra security frame for distributed wireless sensor networks.

2. SECURITY THREADS

There are number of different threats to the sensor networks like DoS, Eavesdropping, Message injection, Message replay, message modification, malicious code, side channel analysis, etc. The security primitives against these attacks are message confidentiality, authentication, service availability, message freshness, message integrity, non-repudiation, intrusion detection, audit trials etc.

In a wireless sensor network it is much easier to monitor transmission between nodes as compared to wired networks because of the broadcast nature of transmission. Encrypting communication between sensor nodes can partly solve this problem but it requires robust key exchange and distribution scheme, compelling the wireless sensor networks to maintain secrecy in the rest of the network when an adversary compromises few sensor nodes and exposes their secret keys.

In Sensor networks end-to-end encryption is impractical because of large number of communicating nodes and each node is incapable of storing large number of encryption keys. Therefore hop-by-hop encryption mechanism is usually used in which each sensor node stores only encryption keys shared with its immediate neighbors [5].

A DOS attack is an event that causes weaken or reduces the network's capacity to carry out its expected function. Protocols or design level vulnerabilities are the main cause of DOS attacks. Normally DOS attacks in wireless networks can occur at the physical layer, for example, via radio jamming. Through malicious transmission they can interfere with sensor network protocols or physically destroy central network nodes. "Attackers can induce battery exhaustion in sensor nodes"[6]— for example, they can engage certain specific nodes in processing and forwarding maliciously sent packets, thereby exhausting their energy resource. More dangerous attacks can occur from inside the sensor network if the attackers can compromise the sensor nodes. For example, they could create routing loops that will sooner or later tire out all nodes in the loop. For DOS attack resistance, attempts have been made on cryptographic authentication mechanisms, but because of the limited resources available to a sensor node make digital signature schemes impractical. General DOS attacks are listed in table 1.

Table 1: DoS Attacks

OSI Layer	Attacks
Physical	Tampering, Jamming
Data link	Collision, Exhaustion and Unfairness
Network	Homing, misdirection, Black holes
Transport	Flooding and de-synchronization

Wireless Sensor networks are susceptible to many types of intrusion such as black hole, flooding, misdirection, tempering etc. In wired networks traffic is analyzed at various concentration points for detecting intrusion that requires high memory and consumes lot of energy. Therefore wireless sensor networks require a solution that is fully distributed and inexpensive in terms of memory, communications and energy requirements [7].

3. SECURITY REQUIREMENTS

Basic security services which are generally required, are mentioned below

- **Authentication:** this service is used to ensure that the message originated from authenticated sources, and both communicating entities are legitimate.
- **Access Control:** this service is used to ensure that only authorized entities can access required resources.
- **Non-repudiation:** this service prevents the sender or receiver from denying the sent or received message.
- **Data integrity:** This service ensures that the message is received without modification, or duplication.
- **Data Confidentiality:** data must be sent in an encrypted manner so that no one other than the sender or recipient can read it.
- **Availability:** this service is used to prevent the loss of access e.g. due to denial of service attacks.

4. COMPARISON OF SECURITY PROTOCOLS

Quite Recently some security solutions has been proposed in [8, 9, 10, 11,12] specially for wireless sensor network but each one suffer from various limitations. Adrain Perrig et. al [8] have proposed security protocols suite called SPINS for wireless sensor networks. SPINS consist of two building blocks SNEP and uTESLA. SNEP provides data confidentiality, two party data authentication and data freshness where as uTESLA provides authenticated broadcast for severally resource constraint environment. For data confidentiality they use symmetric encryption mechanism in which secret key called master key is shared between sensor node and base station. SNEP uses one time encryption key that produces from the unique master key. SNEP uses MAC function for two party authentications and checking data integrity. SPINS is based on binary security model means either it provides maximum security or no security. There are number of drawbacks associated with SPINS such as

- SPINS has scalability issue because in there approach number of secret keys is directly proportional to the number of nodes in the network.
- It can only work in non-anonymous environment in which all nodes have some unique id.

- Because of the usage of source routing scheme in SPINS they are making the network vulnerable to traffic analysis [13].
- It does not address security in the Physical layer therefore they are unable to provide defense mechanism against physical layer attacks such as jamming etc [10].

K. Jones et. al [10] have proposed a solution for providing differential security services for wireless sensor network by using parameterized frequency hopping and cryptographic keys mechanism. Their solution provides integrity, confidentiality and availability for the sensor networks that consist of anonymous nodes. In order to ensure the availability they use frequency hopping scheme that is conventionally used for “implementing frequency diversity and interference averaging in a non-hostile environment”. Due to the node anonymity there solutions does not provide access control and non-repudiation. They do not provide direct authentication mechanism but on the other hand it is very difficult for the external node who attempt to masquerade as a legitimate node. The main reason for this is that it is very difficult for intruder to guess which set of frequencies and hopping sequence is currently used [14].

Chris Karlof et. al [9] have proposed TenySec architecture for wireless sensor networks. TenySec is a link layer security protocol that provides authentication, integrity and confidentiality by adding less than 10% of energy, latency and bandwidth overhead. TenySec does not provide access control and non-repudiation. It also does not provide protection against physical layer attacks. The major drawback of this solution is that it is tightly coupled with Berkeley TenyOS and can not be use for general sensor network model [7]. Like SPINs it can only work in non-anonymous environment in which all nodes have some unique id.

Taejoon park and Kang G. Shin [11] have proposed Light weight Security protocol (LiSP) that’s makes a tradeoff between security and energy consumption through efficient re-keying mechanism. LiSP achieves authentication, confidentiality, data integrity, access control and availability. Another important feature of LiSP architecture is the ability to detection intrusions. By using LiSP each node need to save eight keys.

Sencun Zhu et. al [1212] have proposed Localized Encryption and Authentication protocol (LEAP) for large scale distributed wireless sensor networks. The unique feature about LEAP is that, it they provides four key mechanisms in order to meet different security requirements and their keys mechanism is scalable. The major draw back of that LEAP is that it only works in static environment in which nodes are not mobile, and also author assumes that the Base station will not be compromised.

General Comparison of all above discussed schemes from security parameters perspective is given in Table 2.

Table 2: Comparison of Security Protocols for WSN

	SPINS	Tiny Sec	Freq Hopping	LiSP	LEAP
Authentication	✓	✓	✗	✓	✓
Access Control	✗	✗	✗	✓	✗
Non-repudiation	✗	✗	✗	✗	✗
Integrity	✓	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓	✓
Availability	✗	✗	✓	✓	✗

5. TETRA SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS

Our Tetra security framework consist of four main components

- Light weight Key Management Scheme (LKMS)
- Light weight Secure Routing Protocol (LSRP)
- Light weight Intrusion Detection System (LIDS)
- Light weight Trust Management System (LTMS)

Here term ‘light weight’ means procedures would take less computation power and consume less energy. All fours components jointly work together to achieve higher security in an efficient manner. They are used to defend most of the passive and active attacks. This Tetra security frame work will be installed in a sink node or base station. In ubiquitous sensor nets, the role of traditional base station is changed to router [15,16]. Tetra will established secure tunnels with user in order to provide services in a secure manner. The scenario is illustrated in fig 1.

5.1 Light weight Key Management Scheme (LKMS)

Generally we talk about how to ensure confidentiality, authentication, and availability etc, but all these services are dependent upon key management. If our key management scheme is not secure them we can not provide secure communication medium. Traditional public key certificate based key management schemes are unsuitable for wireless sensor networks because they are not communication efficient. There are two types of techniques generally used for key management that are interactive schemes and non-interactive schemes [17].

1. Interactive schemes such as elliptic curve cryptography (ECC) approach reduce communication and computations cost but it requires higher interactive exchanges.
2. Non-iterative schemes that used identity based cryptography are still immature and required considerable computations whereas random key pre-

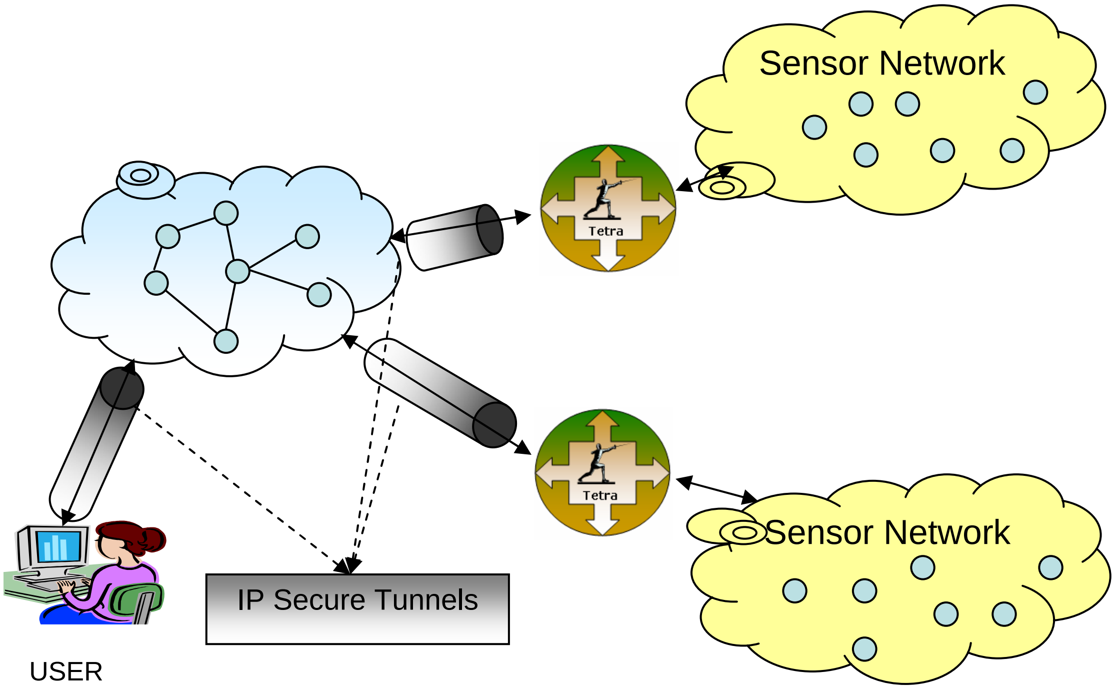

Fig 1: General Scenario of Tetra Security Framework

distribution technique reduces computations at the cost of interactions.

Our goal is to build LKMS that combines the benefits of both, identity based and random based pre-distribution technique called identity based random key pre-distribution scheme (IBRKP). LKMS, by using IBRKP technique established pair wise keys with virtually no extra communications.

5.2 Light weight Secure Routing Protocol (LSRP)

Routing in wireless sensor networks has been reasonably studied by different researcher specially with respect to energy efficient routing. Number of different network routing protocols for wireless sensor networks have been developed such as TinyOS beaconing protocol [18], Greedy Perimeter Stateless Routing (GPSR) protocol [19], Geographical and energy aware routing protocol (GEAR) [20], Low-energy adaptive clustering hierarchy (LEACH) protocol [21], Threshold sensitive Energy Efficient sensor Network protocol(TEEN) [22],Power-Efficient GAthering in Sensor Information Systems, (PEGASIS) [23], and some other energy conserving topology maintenance protocols such as SPAN [24], GAF[25] and AFECA[26].

All these protocols have not been designed keeping security in mind therefore they are vulnerable to many types of attacks such as bogus routing information, elective forwarding, Sybil, hello floods, worm holes etc. Table 3 shows the summary of attacks against proposed sensor network routing protocols [27]. From this table it is clear that most of the routing protocols are insecure.

Table 3: Attacks against Routing Protocols of WSN

(✓: Possible, ✗: Not Possible)

Attacks **Routing Protocols**	**Bogus routing information**	**elective forwarding**	**Sybil**	**HELLO floods**	**Worm holes**
TinyOS beaconing Protocol	✓	✓	✓	✓	✓
Geographic routing protocol (GPSR, GEAR)	✓	✓	✓	✗	✗
Clustering based protocols (LEACH, TEEN, PEGASIS)	✗	✓	✗	✓	✗
Energy conserving topology maintenance protocols (SPAN, GAF, AFECA)	✓	✗	✓	✓	✗

The objective of LSRP is to build secure routing protocol that shows resistance to all types of active and passive attackes. LSRP will be build by following the guidelines that have been suggested by Charis Karlof and David Wagner in [27] for designing secure routing protocols.

5.3 Light weight Intrusion Detection System (LIDS)

Detection of intrusion in wireless sensor network is very difficult because of specific constraints. We need solution that is fully distributed and requires less computation and communication overhead. That is the objective of LIDS system. We need LIDS systems in order to detect that node has not been compromised as well as no node will be able to send false data.

5.4 Light weight Trust Management System (LTMS)

With the emergence of ubiquitous computing the need of trust management is also increased. Current research on sensor networks is mostly built on a trusted environment [28]. Before implementing any security mechanism we need to ensure that all nodes are trusted. Trust can solve the problems that can not be solved by traditional cryptography security [29] for example, judging the quality of sensor nodes and the quality of their services, and providing the corresponding access control, e.g., does the data aggregator do the aggregation correctly? Does the forwarder send out the packet in a timely fashion? Traditional Trust mechanisms are not suitable in wireless sensor networks because of limited resources. Therefore we need Light weight Trust management System (LTMS) for large scale distributed wireless sensor networks.

6. CONCLUSION

In this paper we have investigated the current security solutions for wireless sensor networks and find outs their major pros and cons. Initially we have given the comparison of various security protocols from the perspective of basic security parameters such as authentication, access control, non-repudiation, integrity, confidentiality and availability. We found that none of the solutions provides complete security and most of them are vulnerable to many types of security threats. There are still many open problems exists. Therefore we have proposed new Tetra security framework in order to achieve highest level security and energy efficiency for ubiquitous wireless sensor networks.

7. REFERENCES

1. S. Tilak, N. B. Abu-Ghazaleh and W. Heinzelman, “Taxonomy of Sensor Network Communication Models", Mobile Computing and Communication Review 6(2): 1-8, Apr 2002
2. Ian F. Akyildiz, Weilian Su, Yogesh S., and Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communications Magazine, Aug 2002
3. Nadeem Ahmed, Salil S. Kanhere, Sanjay Jha, “The holes problem in wireless sensor networks: a survey”, ACM SIGMOBILE Mobile Computing and Communications Review, Volume 9 , Issue 2, April 2005, pp. 4-18
4. M. Perillo and W. Heinzelman, "Wireless Sensor Network Protocols," To appear in Fundamental Algorithms and Protocols for Wireless and Mobile Networks, CRC Hall, 2005
5. H. Chan and A Perrig. “Security and Privacy in Sensor Networks”, IEEE Computer 36(10), Oct 2003, pp. 103-105.
6. Anthonay D. Wood, John A. Stankovic, “Denial of Service in sensor network”, IEEE Computer, 35(10), Oct 2002, pp. 54-62
7. Adrain Perrig, John Stankovic, and David Wagner, “Security in wireless sensor networks”, communications of ACM, Vol 47(6), Jun 2004, pp. 53-57
8. A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, “SPINS: Security protocols for sensor networks”, proceedings of 7th annual international conference on Mobile computing and networking, Rome, Italy, Aug 2001, pp 188-189
9. Chris Karlof, Naveen Sastry, and David Wagner, “TinySec: a link layer security architecture for wireless sensor networks”, Proceedings of the 2nd international conference on Embedded networked sensor systems , Baltimore, MD, USA, Nov 2004, pp 162-175
10. K. Jones, A.Wadaa, S. Oladu, L. W|son, and M. Etoweissy, “Towards a new paradigm for securing wireless sensor networks”, Proceedings of the 2003 workshop on New security paradigms, Ascona, Switzerland, Aug 2003, pp 115 - 121
11. Taejoon Park, and Kang G. Shin, “LiSP: A Lightweight Security Protocol for Wireless Sensor Networks’ ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, Aug 2004, Pages 634–660
12. Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, “LEAP: Efficient Security Mechansim for Large-Scale Distributed Sensor Networks ”, Proceedings of the 10th ACM conference on Computer and communications security, Washington, USA, 2003, pp. 62-72
13. Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, and John Pinkston, “Security for Sensor Networks”, Proceeding of 2002 CADIP Research Symposium, Baltimore, MD, Oct 2002.
14. Stephan Olariu, Ashraf Wada, Larry Wilso, and Mohamed Eltoweissy, “Wireless Sensor Networks: Leveraging the virtual infrastructure”, IEEE Networks, vol 18(4), July 2004, pp. 51-56
15. Shu Lei, Wang Jin, Xu Hui, Jinsung Cho, and Sungyoung Lee, “Connecting Sensor Networks with TCP/IP Network”, International Workshop on Sensor Networks (IWSN'06) in conjunction with APWeb 2006 , Harbin, China , Jan 16-18, 2006
16. A. Dunkels, J. Alonso, T. Voigt, H. Ritter, J. Schiller, “Connecting Wireless Sensornets with TCP/IP Networks”, In Proceedings of WWIC2004, Germany, Feb 2004.
17. David W. Carman, “New directions in Sensor Network Key Management”, International Journal of Distrinuted Sensor Networks, 1:3-15, 2005
18. Jason Hill, Robert Szewczyk, Alec Woo, Seth Hollar, David Culler, and Kristofer Pister, "System architecture directions for networked sensors," in Proceedings of the 9th international conference on Architectural support for programming languages and operating systems, 2000, pp. 93-104
19. B Karp, HT Kung, “GPSR: greedy perimeter stateless routing for wireless networks”, Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, USA, 2000, pp. 243-254
20. Yan Yu, R Govindan, D Estrin, “Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks,” Univ. California, Los Angeles, Tech. Rep. UCLA/CSD-TR-01-0023, 2001.

21. Wendi B. Heinzelman,Anantha P. Chandrakasan, and Hari Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks”, IEEE Transactions On Wirless communications vol 1(4), Oct 2002, pp. 660-670
22. Arati Manjeshwar, Dharma P. Agrawal, and Hari Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks”, IEEE Transactions on Wireless Communications, vol. 1(4) Oct 2002, pp. 660–670,
23. S Lindsey, CS Raghavendra, S Raghavendra, “PEGASIS-Power-Efficient GAthering in Sensor Information Systems”, Proceedings of IEEE Aerospace Conference, vol 3, , 2002, pp. 1125-1130
24. Benjie Chen, Kyle Jamieson, Hari Balakrishnan and Robert Morris, “Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks”, Wireless Networks, Vol 8(5), Sep 2002, pp. 481-494
25. Y. Xu, J. Heidemann, and D. Estrin, “Geography Informed Energy Conservation for Ad Hoc Routing”, MOBICOM 2001
26. Y. Xu, J. Heidemann, and D. Destrin, “Adaptive Energy-Conserving Routing for Multihop Ad Hoc Networks”, USC/ISI Research Report 527, October, 2000.
27. C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Ad Hoc Networks. vol 1(1), 2003, pp. 293-315
28. Elaine Shi and Adrian Perrig, “Designing Secure Sensor Networks”, IEEE Wireless Communications, Dec 2004, pp. 38-43
29. John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, “Wireless sensor network security: A Survey”, Technical Report MIST-TR-2005-007, July, 2005