Enhanced Security in Wireless Sensor Networks

Siddharth Rao
Aalto University School of Science
siddharth.rao@aalto.fi

Abstract

Increased demand for Wireless Sensor Networks(WSNs) in fields such as the military, ecological survey and health related areas which deals with sensitive information has imposed the overhead of security in such networks. Attacks on wireless sensor networks have justified the importance of security in this field. Constraints on memory, computation, energy and transmission range associated with WSNs makes security a challenging task to implement. This paper mainly discusses the security aspects of wireless sensor networks in terms of cryptographic implementations and secure routing strategies based on the survey and researches made with emphasis on the architectural limitations of sensor nodes. This paper also discusses the scientific methods involved in each of the chosen strategies by comparing, analysing and evaluating them.

Keywords: Security in Wireless Sensor Networks, Cryptographic Implementations, Experimental Analysis , Secure Routing Strategies, Simulation Studies.

1 Introduction

Wireless sensor nodes are the tiny sensing devices dispersed over a specific geographical area of coverage, which can sense changes in physical and environmental parameters such as temperature, pressure , humidity and sound. Such nodes are capable of communicating with similar devices in the vicinity of the same coverage zone for purposes such as target tracking, environmental monitoring and surveillance. A network consisting of all such nodes having hardware, software and operating system within it, is known as Wireless Sensor Network. The applications of such networks can be seen in many fields such as agriculture (where WSN is used to control the temperature and humidity levels), burglar alarm systems in new age homes, prevention of natural disasters, air pollution monitoring, health care, etc. Modern day WSNs are also capable of measuring and hence monitoring soil makeup, noise levels, vehicular movements, lighting conditions, presence/absence of objects, mechanical stress level, etc. Because of its applications in diversified domains such as military, ecological surveys and health monitoring which often deals with monitoring sensitive information, security has become the crucial feature of Wireless Sensor Networks.

2 Background

Wireless Sensor Networks consists of myriads of nodes which are densely spread over a field and they send all the data that they sense/measure to a base station, from which it can be made available to the intended end users. Every sensor node in the network consists of four different parts namely sensing unit, processing unit , transceiver unit and power unit. The sensing unit is responsible for sensing physical/environmental parameters like temperature and pressure ; the processing unit processes the data based on the information being sensed ; the transceiver unit looks after the transmission of processed data to the base station or to some other node in the network; and the power unit supplies power required for the working of a sensor node. A schematic representation of the Wireless Sensor Network can be seen in Figure 1. Various layers of network protocols that can be implemented in the sensor nodes are physical layer, data-link layer, network layer, transport layer and application layer. Unlike the typical OSI model implementation in any large scale computing systems, there is no presentation layer and session layer. The presentation layer is responsible for encrypting the data and session layer takes care of authentication / authorization of the connection. To achieve required amount of security in WSNs, these functionalities should be performed by any of the other protocol layers or by the hardware unit of the sensor nodes.

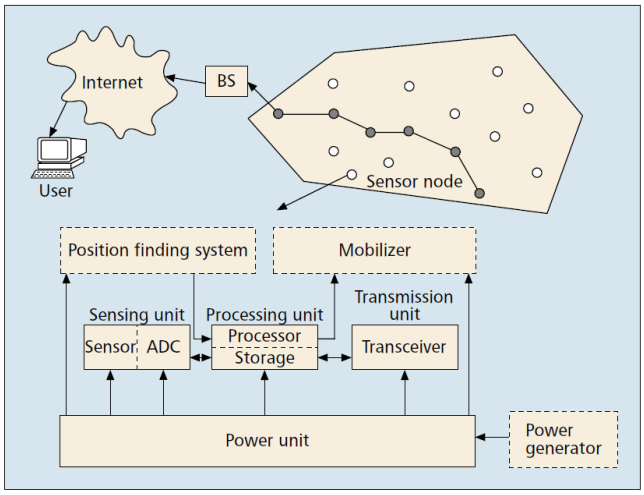

Figure 1: Architecure of WSN [5]

2.1 Security Requirements and Constraints

WSNs should achieve the security goals such as availability, authorization, authentication, confidentiality and non-repudiation like any other systems. Along with these, maintaining the freshness, forward and backward secrecy are the additional security goals to achieve good level of security. Freshness is a property by which the replaying of old data by the attacker can be restricted. Forward secrecy refers to the fact that once the node is disconnected from the network, it should not receive any data from the network further. Backward secrecy refers to the rule of thumb that when a new node joins the network, it should not be able to read the earlier transmitted message.

Limitations in terms of availability of energy and physical size of WSN has become a major challenge to implement security in WSNs.One has to pay attention to constraints such as computation, less memory for processing(RAM) and for storage(Flash). Because of these limitations it is not feasible to implement any strong security measure such as a strong encryption scheme in WSNs. Experimental analysis proves that data transmission is very expensive compared to data processing in terms of energy[1]. These facts restricts the use of strong keys to be exchanged between the nodes.

3 Implementation of Cryptography

Since most of the security services in WSNs are ensured by cryptography, it is very important to choose the right kind of cryptographic algorithm to be implemented by considering the constraints such as code, data size, processing time and power consumption. Because of these constraints it is quite infeasible to implement strong cryptographic algorithms such as Diffies-Hellman for key exchange and RSA algorithm for actual encryption. Public Key algorithms like RSA consumes more energy as well as more time because of the complexity in calculations though it can combat against DoS attacks efficiently. Though it is infeasible to implement public key cryptography in WSN, recent researches in this direction has shown that it is implementable by choosing the right algorithm which consumes less energy(by using optimized parameters) , especially with the help of Ecliptic Curve Cryptography(ECC). ECC provides almost equal amount of security compared to RSA but with smaller key size and less computational complexity for the processor of a sensor node. For example: ECC- 160 provides equal security compared to RSA-1024 which is now considered as the accepted level of security for many applications. Similarly the same amount of security can be achieved from ECC-224 from that of RSA-2048.

Though public key cryptography is feasible in WSNs, as it consumes more power and requires more computation, researches have been made on implementing symmetric key cryptography. It is found that symmetric key cryptography is faster and more energy efficient compared to most of the the asymmetric cryptographic implementations. However the problem with symmetric cryptography is that the key management is not an easy task [2].

3.1 Experimental Analysis

Experiments with Ecliptic Curve Cryptography in comparison to RSA implementations on WSNs with different key spaces prove that ECC is more feasible for WSN as it consumes less power and faster than RSA. The experiments are based on ATmega128 processor as well and on Mica2 motes with TinyOS as the operating system in the senor nodes. The energy required for digital signature and key exchange is also considered with the assumption that private key operations will be performed by the base station or a third party but not by the sensor node itself.

For experiments on symmetric key cryptography [5] popular encryption schemes like RC4, RC5, SHA-1, MD5, Rijndael, MISTY1, KASUMI were evaluated on six different sensor node architecture ranging in window size from 8 bit (Atmel AVR) to 32 bit(Strong ARM, Xscale).Though RC5 and RC6 are selected as encryption schemes by many works, as per the experimental analysis, Rijndael is suitable for high security and energy efficiency, while MISTY1 is found to be suitable for good storage along with having energy efficiency.

The results [5] shows that Operation time of ECC- 160 is 0.81 seconds where as that of RSA- 1024 with private key is 10.99 seconds. ECC -224 operates within 2.19 seconds, and RSA -2048 takes as high as 83.26 seconds. Even though the asymmetric cryptography implementations display good results in terms of speed, they are not energy efficient when compared to their symmetric cryptographic counterparts. So symmetric cryptography has been the main area of focus. The key distribution problems associated with such implementations can be resolved by using pre-distribution of the keys.

4 Secure Routing mechanism

Encryption and secure approach for key exchange are not enough to defend WSNs from very frequent and common attacks such as denial of service and compromised node(black holes). Because, if one node is compromised , the attacker can learn about the encryption scheme and have access to the keys. In worst cases, the attacker can at least jam the traffic through that node even without the knowledge of encryption or decryption. The solution to such situation is to exploit the routing mechanism of the network. Usually the routes are calculated in a deterministic way. Even if the routes are based on a random approach (Wanderer's algorithm), they are neither efficient nor secure. So a secure randomized routing algorithm would add extra layers of security to the existing model of WSNs.

The ideal approach to build a secure randomized route is to make it as dispersive as possible. The whole mechanism can be considered as a two-fold process. The first step is to divide the message into multiple shares. Next step is to send the shares through different nodes which are widely dispersed. The rule of thumb associated with dividing the message (into say M shares) is that the original message can be recovered from the combination of at least T shares ; but no information is retrieved from even one less than T shares. The goal of second step is to achieve a mere random routing

mechanism in a way that the attacker has no information to guess the next node and he cannot trace the routing mechanism. Depending on the type of data that has to be sent from the node, there are four randomized dispersive routing mechanisms have been developed by Tuo Shu et. Al . They are Purely Random Propagation (PRP); Non Repetitive Random Propagation (NRRP); Directed Random Propagation (DRP) ; Multi cast Tree -assisted Random Propagation (MTRP). These methods differ in the way they choose their next node while traversing.

Apart from this approach, many secure routing algorithms have been proposed based on hierarchical sensor networks. But most of them fail to show the effects of energy consumption due to different cluster size [2]. Some of them may ease the secure routing issues, but they complicate the route and cluster management along with increasing the transmission cost.

4.1 Simulation studies

The research by Tao Shu et.al [4] is based on the simulation where the simulation experiment is conducted on all four proposed randomized routing protocols. The simulation set up is such that it mimics the real world scenarios and the results are compared with the deterministic routing mechanism counterpart H-SPREAD. The performance is based on the interception probability , which is defined as the ratio of number of message shares sent from a node to the number of message shares received by the base station which is sufficient enough to circumvent the blackholes. Also the hop count is taken into consideration because it indirectly influences the performance. The results from simulation shows that the security in WSN is increased in PRP, DRP, NRRP and MTRP with no or negligible decrease in performance when compared to H-SPREAD.

5 Discussion and Comparison

The experimental analysis of different cryptographic implementations on various architecture gives a clear insight about the behaviour of the algorithms. But the decision about selecting the appropriate cryptographic scheme depends on the computation and communication capacity of the sensor node. Though experiments show that asymmetric cryptography can be implemented in WSNs, they consume more energy. Symmetric key cryptography is better in terms of speed and energy cost compared to that of asymmetric cryptography. More efforts on efficient and flexible key distribution mechanism might solve the issue. Along with that powerful motes should be designed in order to provide high level of security through cryptography in Wireless Sensor Networks.

The secure routing mechanism discussed in this paper is effective in terms of combating against DoS and blackhole attacks. The packet loss due to those attacks can be lowered at a magnitude of 10^{-3} by using randomized dispersive routing mechanisms. However the research by Tao Shu et.al. does not address the problem arising from those mechanisms such as need for additional memory in the header of the message share which in turn will result an expensive communication. The real time scenarios are quite not as same as the simulation studies. The network topology changes frequently and error messages are produced normally. Unauthorized nodes can produce similar messages and most of the researches done in this direction, fail to address this problem.

Using Tiny Active Message(TAM) facility of TinyOS with encryption for key exchange would be an optimal way to achieve a good level of security when symmetric cryptography is implemented. This can be made even more secure by using the randomized dispersive routing mechanism over an encrypted channel with TAM.

6 Conclusion

The increasing demand of security in WSNs because of its applications in fields such as military have imposed strict requirement of security. Also the attacks on WSNs have proved that security loopholes may effect serious damage to the sensitivity of the data being fetched. There is a famous quotation about cryptography that reads as “Whoever thinks his problem can be solved using cryptography, does not understand the problem and does not understand cryptography” (attributed to Roger Needham and Butler Lampson). Cryptography alone can not be a complete solution to achieve security. Usage of appropriate cryptographic schemes along with secure routing mechanisms using randomized dispersive routes (which are independent of the underlying cryptography) shows great increase in security, but more research has to be done in order to overcome the limitations of WSNs. Though it is not possible to generalize the security implementations by having same set of security measures in all the WSNs as they have different capacity and architecture, the holistic view of security [3] should be taken into consideration by protecting all the layers of wireless sensor networks.

References

[1] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, 7(3):537–568, 2009.

[2] X. Chen, K. Makki, K. Yen, and N. Pissinou. Sensor network security: a survey. *Communications Surveys & Tutorials, IEEE*, 11(2):52–73, 2009.

[3] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong. Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, volume 2, pages 6–pp. IEEE, 2006.

[4] T. Shu, M. Krunz, and S. Liu. Secure data collection in wireless sensor networks using randomized dispersive routes. *Mobile Computing, IEEE Transactions on*, 9(7):941–954, 2010.

[5] Y. Wang, G. Attebury, and B. Ramamurthy. A survey of security issues in wireless sensor networks. 2006.