ISSN No. 0976-5697

Volume 7, No. 6 (Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARITCLE

Available Online at www.ijarcs.info

Requirements and Challenges in Wireless Sensor Network Security

Nitika Goyal,
Deptt of Computer Sience,
Guru Nanak College, Budhlada(Mansa)

Satveer Kaur
Deptt of Computer Sience,
Dashmesh College, Zirkpur

Abstract:*The need of a powerful security mechanism has become essential, with the rapid growth of wireless sensor network. Since these networks may deal with confidential information or work in unfriendly unattended situations, it becomes extremely important that such security issues be strongly dealt withright from the system design phase. It is true that wireless sensor networks face issues which are totally different from that of customary networks because of restricted resources. Due to great potential of research, sensor networks have become hot topic for researchers. Keeping all these things in mind, we are trying to review the significant aspectsofsecurity of sensor network, and figure out the hindrances and prerequisites in wireless sensor security.*

INTRODUCTION

Wireless sensor networks are rapidly picking up prevalence because they providesolutions which are economically feasible [1]. Being economical, huge sensor clusters can be deployed for military as well ascivilianapplications. At the same time sensor networks face problems of restricted storage capacity and power shortage. Both of these problems restrict the use of customary network security techniques in wireless sensor networks.

Network security becomes even more challenging due to unreliable communication channel and unattended operations. Without a doubt, most of the wireless sensors have the features of decade old machines and the challenge before industry is to cut the sensor without affecting its processing power. In view of that, theresearchers have started to workingon how to increase the computing capabilities of wireless sensor nodes while dealing with the security attacks effectively.

Each and every aspect of the wireless sensor network is being inspected including cost-effective and secure routing, data aggregation etc. Notwithstanding those customary security issues, we see that generallymost of the sensor network techniquesconsider the sensor nodes secure and cooperative. However this is not true as most of the wireless sensor networking applications need a specific measure of trust in the application so as to keep up legitimate network function. Thus researchers have started thinking beyond the cryptographic techniques and are trying to build an innovative sensor trust model. Many attacks are specifically designed keeping in mind the two major weaknesses of wireless sensor networks i.e. unattended operation and non-reliable communication.

The major aspects of security of wireless sensor network have been discussed here: the challenges in sensor network security and the requirements of a secure wireless sensor network.

CHALLENGES IN SENSOR SECURITY

Being a special network, the wireless sensor network has numerous limitations contrasted with a conventional computer network. So it has become hard to specifically utilize the current security techniques to deal with the obstaclesin security of wireless sensor networks. Howeversome valuable security techniques can be developed by acquiring the ideas from present security mechanisms.But we have to first understand the obstacles in sensor security for this.

Extremely_LIMITED_RESOURCES

The very first requirement of every security techniqueis resources like enough power supply to energize the sensor, storage space etc. But a small wireless sensor is not capable of providing such resources

• Limited Memory :A sensor is a modest gadget with low storage capacity. So size of the security algorithm is restricted. Generally a sensor has a 16-bit, 8 MHz RISC CPU with just 10K RAM, 48K memory, and 1024K flash storage. With this configuration, one needs to compromise with the size of software to be built for such sensor thus affecting the security of wireless sensor network.

• Restricted Power: One of the biggest weaknesses of wireless sensor is energy. The sensors of a wireless sensor network can't be easily replaced due to it their high cost. So there is a dire need of conserving the energy of sensors which will indeed increase the life of entire sensor network. The power reserve of a sensor must be kept in mind while implementing a security mechanism.

Before implementing a security mechanism to a sensor it should be taken care of that the lifespan of sensor should not get affected as the security mechanisms consume extra power during the processing of various security functions.

COMMUNICATION

The major threat to security of a sensor is by unreliable communication. The network security depends intensely on defined protocol, which further relies on upon communication.

• Non-reliable Transfer: The sensor network uses connectionless packet based technique for routing thus the transfers are highly unreliable. Exceptionally congested hubs or errors in communication channels may result in missing or damaged packets. More resources are devoted to error handling due to very high channel error rate.Sensitive security packets (e.g. containing cryptographic key) might also be lost if error handling provisions are not made. This may incorporate, for instance, a cryptographic key.

• Conflicts: The communication may still be unreliable even if the channel is reliable..The reason behind it is that the wireless sensor network uses broadcasting method for communication. Conflicts occur on collision of two packets which results in failure of transfer process. This is the main issue in congested wireless sensor network.

• Latency: There is latency in wireless sensor network due to network traffic and multi-hop routing. Thus it becomes hard to synchronize sensor nodes. The synchronization problemis important for sensor security where the security system depends on distribution of cryptographic keys or critical event reporting.

UNATTENDED OPERATION

A sensor node may remain unattended due to function of a specific sensor network . There are three principal issues with unattended sensor nodes:

• Prone to Physical Attacks: The operating environment of a sensor may be open to terrible climate conditions, adversaries etc. The probability that a sensor endures a physical attack in such conditionsis much higher than that of a computer installed at a safe zone.

•

Managed Remotely: Remotelymanaged sensor network makes it practically difficult to recognize physical tampering and maintenanceproblems e.g. replacement of battery. A classy example of such case is a sensor nodeapplication for remote observation missions across enemy lines.

• Lack of centralized management: A sensor network ought to be a distributed network with no centralized management. So any loophole in the design of sensors makes the organization of network troublesomeand inefficient.

SECURITY REQUIREMENTS

A sensor network is an extraordinary network whichwhile being similar to the traditional computer network,hasits own exceptional prerequisites. In this manner, wireless sensor network requirements are amalgamation of incorporating both the prerequisites of a traditional networkas well aswireless sensor network specific exclusive requirements.

INFORMATION PRIVACY

One of the most essential issues in network security is Information privacy. Any security centered network willgenerally handle this problem first of all. The main security issues related to data confidentiality are listed below:

• The neighboring sensors should not get access to sensor readings. Particularly in sensitive applications like military application, information security is very important.

• Most of the times confidential data (e.g. key distribution) is exchanged by the sensor nodes. Thus a secure wireless sensor network is essential for secure communication.

• Even public keys need to be encrypted as they are also prone to attacks.

Encryption technique with the help of a confidential keyis used to keep the information protected from the access of attacker.

DATA INTEGRITY

We can protect data from attackers by implementing confidentiality techniques. But it does not guarantee the safety of data. The attackers can modify the information, in order to generate chaos in the sensor network. For instance, data can be manipulated by any faulty node and the manipulated packet can be delivered to the recipient instead of the original one. Malicious node is not the only factor responsible for data loss;communication environmental factors also lead to loss of data. Thus the aim of data integrity is to ensure that information doesn’t get manipulated during transfer process.[2]

DATA FRESHNESS

Beside data integrity and confidentiality, we should also refresh the data from time to time. It ensures that the data is latest and no old message has been repeated. . Data freshness becomes even more if keys are shared in the network. Traditionally values of shared keys should be changed after some time.[3] Due to the time taken in propagating the shared key to entire network, the attacker gets a chance to repeat the attack.. Additionally, it is anything but difficult to disturb the ordinary work of the sensor, if the sensor is ignorant of the new key change time. To dal with this issue a timerneed to be attached to the packet to make sure that the data is fresh.

AVAILABILITY

Altering the conventional encryption methods to make them suitable for the wireless sensor network requires some additional expenses. Some methodologies prefer code modification to reuse the code again and again. Some other methodologies utilize extra communication to accomplish the same objective. Rest of the methodologies enforce constraints on access of data, or implement an inadmissible plan for simplification of algorithms. Thus, these methodologies affect the availability of sensor in one or other way. Some of which are listed below:

- Extra energy is required for extra computations. The data will be lost if there is no more energy

- Additional communication expends extra energy. Probability of conflict also increases with increase in communication.

- Being a centralized system, chances of single point failure are very high

SELF-ORGANIZATION

Being a temporary network, wireless sensor network needs all sensors to work independently. Each sensors in such networks should be flexible enough to organize and modify itself in according to the situation as there is no provision for network management in wireless sensor network. This feature is a great loophole in the wireless sensor network security .

Time synchronization is one of the important pre-requisites of wireless sensor network applications. Sensor radio must be switched off from time to time to save power. In two way communication, delay time of a packet is also calculated by sensors. Group synchronization is also required by certain sensor network applications [4]. Various secure synchronization protocols are used for solving the problem of synchronization.

SECURE LOCALIZATION

The ability to automatically and accurately locate each sensor in the network affects the utility of a sensor network. A sensor network intended to find faults will require precise information about the location for detecting the location of fault. However a non-secured information about locationcan be easily changed by attackers using various techniques.

Onof such techniques is multi-alteration (VM). In this technique, a gadget's location is precisely calculatedusing a series of known reference points. [5] The exact location of a node is guaranteed using authenticated ranging and distance bounding techniques. As a result the attacking node can only extend the reference point to its claimed distance.Along with this, the attacking node needs to prove that its distance is shorter from any other reference point [6]. In this case a node manipulating and localization protocol is found as the attacking node cannot prove this. A three step algorithm SPINE(Secure Positioning for Sensor NEtwork) which is based on multi-alteration is used in large sensor networks[7].

The following assumptions about locators are made:

- The locators are trusted
- Every locator is knows its location.

A beacon information sent by every locator helps a sensor in calculating its location. Every locator broadcasts its location in the form of beacon. A node computes its location by using all the beacons it receives. The calculation is based on the locators’ coordinates. The final calculation results in overlapping antenna region and the center of gravity of this region is taken as the final location [6].

AUTHENTICATION

An attackerdoesn’t onlymodify the packet data;it can modify the sequence of packets by inserting extra packets. Thus the receivershould verify the source of data before using it in decision making. Thus message authentication plays a vital role in sensor networks. It allows thereceiver to confirm that it is the real sender who has sent the data. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys.[8] In a two way communication, the sender and the receiver own a confidential key which is used to calculate MAC(Message Authentication Code) thus paving way for data authentication.

CONCLUSION

We have portrayed three major dimensions of wireless sensor network security: requirements andobstacles. The purpose of this paper is to give both an outline of the fairly wide range of security concerns of wireless security network, and give the references so that further study of the concerned literaturemight be done.Nowdays,wireless sensor networks turn out to be common,so concerns related to security of these networks need to be addressed so that they can be implemented effectively in future. We likewise hope that the present and future work on security and privacy will make wireless sensor networks a more alluring alternative for the coming generations.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks.*IEEE Communications Magazine*, 40(8):102–114, August 2012.

[2] Tin win maw,Myo hein jaw, “ A secure for mitigation of DoS attack in cluster Based wireless sensor networks”, IJCCER , vol. 1,Issue 3,2013

[3] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, year 2002

[4] P. Albers and O. Camp. Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches. In *First International Workshop on Wireless Information Systems, 4th International Conference on Enterprise Information Systems*, 2012.

[5] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In *The Second USENIX Workshop on Electronic Commerce Proceedings*, Oakland, California, 2009.

[6] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In *IWSP: International Workshop on Security Protocols, LNCS*, 2010.

[7] D. Braginsky and D. Estrin. Rumor routing algorthim for sensor networks. In *WSNA ’02: Proceedings of the 1st ACM international workshop on Wirelesssensor networks and applications*, pages 22–31, Newyork, NY, USA, 2012.

[8] Prajeet Sharma, Niresh Sharma, Rajdeep Singh, "A Secure Intrusion detection System against DDOS Attack in Wireless Mobile Ad-hoc Network",IJCA, Vol. 41–No.21, March 2012.