Research Article Impact Factor: 4.226 ISSN: 2319-507X
Anuja A. Dahane, IJPRET, 2016; Volume 4 (9): 1017-1024 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW ON EFFECTIVE SECURITY MECHANISM FOR WIRELESS SENSOR NETWORKS

ANUJA A. DAHANE[1], PROF. ANKIT R.[1]

1. Computer Science and Engineering, Dr. Rajendra Gode Institute of Technology and Research, Amravati, India.
2. Assistance professor, DRGIT&R, Amravati, India.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* As wireless sensor networks are growing fast so they need for effective security mechanisms as well. Sensor networks interact with sensitive data and operate in a hostile unattended environment, hence security concerns be addressed from the beginning of the network design. Due to resource and computing constraints, the biggest challenge in sensor network is to provide security in routing protocols Asymmetric cryptographic algorithms are not suitable for sensor network providing security, as sensor nodes has limited computation, power and storage resources. On the other hand, it is not feasible to replace the batteries of thousands of sensor nodes, hence sensing, computing and communication protocols must be made as energy efficient as possible .We survey on the major topics in secure protocol and routing for wireless sensor network and focus on four recent papers published which also deal with data integrity, authentication, classify different types of attacks and their corresponding countermeasures.

Keywords: Component; Formatting; Style; Styling; Insert

Corresponding Author: MS. ANUJA A. DAHANE

Access Online On:

www.ijpret.com

How to Cite This Article:

Anuja A. Dahane, IJPRET, 2016; Volume 4 (9): 1017-1024

PAPER-QR CODE

INTRODUCTION

A Wireless Sensor Network (WSN) consists of a mass of inexpensive, lightweight, battery-operated multifunctional sensor nodes. The feasibility of these sensor networks is accelerated by the advances in MEMS (Micro ElectroMechanical Systems) technology, combines with low power, low cost Digital Signal Processors (DSPs) and Radio Frequency (RF) circuits. Sensor networks are deployed in military or citizen field for collecting information or monitoring environment. Sensors nodes are severely energy constrained and expected to last until their energy drains out. Since it is not practical to replace the batteries of thousands of sensor nodes, the key challenge in sensor networks becomes to maximizing the lifetime of sensor nodes. Therefore sensing, computing and communication protocols must be made as energy efficient as possible. Another key issue in wireless sensor networks is to have secure communication between sensor nodes and base station. A very few research has been reported in the literature so far on sensor network security. Sensor nodes can also be used in habitat monitoring, energy management, inventory control, and military warfare. Thus many sensor networks will likely to be deployed in open, physically insecure, or even hostile environments where node compromise is a distinct possibility. Depending on the deployment platform, there are a variety of applications for such sensor networks. To provide security, communication in sensor network should be encrypted and authenticated. Researchers therefore began focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security. It is important to prevent unauthorized users from eavesdropping, obstructing and tampering with sensor data, and launching denial-of-service (DOS) attacks against entire network. A secure routing protocol should be such to handle any attack in a way so that network continues to function properly.

II. LITRETURE SURVEY

Many researchers have proposed many different techniques to provide security in ad-hoc wireless networks. The application of these techniques to sensor networks is promising; however the possibility of malicious nodes blackmailing good nodes and the difficulty in distinguishing between node misbehavior and poor network conditions must be handled with care. In the paper [7] the authors Perrig et al. presented two security protocols optimized for use in sensor networks, SNEP and μTESLA. SNEP provides confidentiality, authentication, and freshness between nodes and the sink, and μTESLA provides authenticated broadcast. Both are useful building blocks for securing routing protocols in sensor networks. To achieve efficient key management, several symmetric key based techniques were proposed in the past. To the studies on symmetric key cryptography, recently, there are a number of studies investigating the implementation of PKC (Public Key Cryptography) in sensor networks.

The authors in the paper [1] presented a new taxonomy for the classification of authentication protocols in ad hoc networks. Ad hoc networks can be classified into static and mobile networks. Sensor networks (SensNets) typically are static ad hoc networks. On the other hand, mobile ad hoc networks (MANETs) are autonomous systems of mobile nodes that are free to move at will. A hybrid network may also exist.

From a security standpoint, ad hoc networks face a number of challenges. Attacks may come from anywhere and from all directions [8].

In order to provide network security, support for authentication, confidentiality, integrity, non-repudiation, and access control should be provided. The authors believe that authentication is the cornerstone service, since other services depend on the authentication of communication entities [9]. Authentication supports privacy protection by ensuring that entities verify and validate one another before disclosing any secret information. In addition, it supports confidentiality and access control. In this paper the author’s present taxonomy for the classification of authentication protocols in ad hoc networks. They identify three major criteria for classification, based on a node’s role in the authentication process, the type of credentials used for authentication, and the phase during which the establishment of credentials takes place.

Energy Efficient Security Protocol [Cam et al., 2003] Wireless sensor network consists of thousands of wireless nodes, each having sensing capability. These sensors are operated by extremely low powered battery for their sensing, computation and communication purpose. As the sensors are energy constraints, asymmetric cryptographic algorithms are not suitable for providing security. Therefore symmetric cryptographic algorithm is used to support the sensor network security [7]. Again, these algorithms also compromise security due to limited key length and memory available on the sensors. In the paper [3], the authors proposed an “energy efficient security protocol” by using non-blocking OVSF (Orthogonal Variable Spreading Factor) [13] technique in addition to changing session keys dynamically. The rest of the part of this section will discuss the authors proposed security protocol.

III. Energy Efficient Security Protocol

The authors in [3] considered a cluster-based sensor network where each cluster contains a cluster-head. These cluster-heads are responsible to gather data from their corresponding clusters aggregate and transmit to the base station (sink) as shown in figure 1.

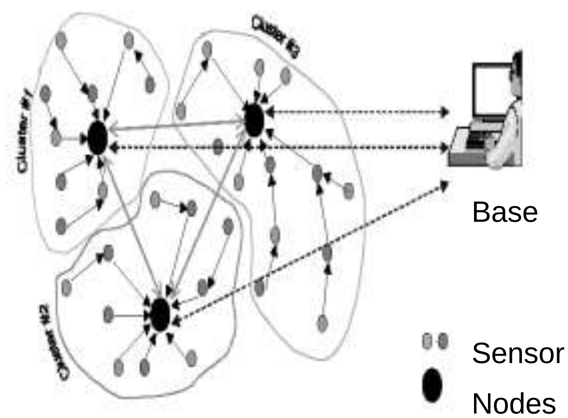

Figure 1: A typical cluster-based sensor network

Sensor nodes are assumed to be immobile and cluster-heads are chosen dynamically from each cluster based on remaining battery power. Base station is assumed to have sufficient power and memory for secure communication with the cluster-heads, other higher cluster heads or external network if necessary. Each sensor nodes are assigned a secret key (Ki) and a unique ID number during the manufacturing phase. Before the network deployment, the base station is given all the ID numbers and Ki of the nodes belongs to it. Base station also generates a session key (Kb) at a certain time intervals and broadcasts to all the sensor nodes. After receiving the session key (Kb), each sensor re-generates their new secret session key (Ki, b) by XORing Ki with Kb. These secret session keys provide a substantial security in sensor networks.

IV.EFFICIENT DISTRIBUTED TRUST MODEL

- **Definition and Properties of Trust**

There are several definitions given to trust in the literature [10]. Trust is always defined by reliability, utility, availability, risk, quality of services and other concepts. Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviours. That is, the trust value is used to reflect whether a sensor node is willing and able to act normally in WSNs. In this paper, a trust value ranges from 0 to 1. A value of 1 means completely trustworthy and 0 means the opposite. Direct trust: Direct trust is a kind of trust calculated based on the direct communication behaviours. It reflects the trust relationship between two neighbour nodes. Recommendation trust: the recommendations from third parties are not always reliable, we need an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust. Indirect trust: When a subject node cannot directly observe an object nodes' communication behaviours, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes.

Based on [11] and [12], we can conclude that there are three main properties of trust: asymmetry, transitivity and composability. Asymmetry implies that if node A trusts node B, it does not necessarily mean that node B trusts node A. Transitivity means the trust value can be passed along a path of trusted nodes. If node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level. Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value.

- **The Calculation of Direct Trust**

Unlike prior work, we compose our direct trust by considering communication trust, energy trust and data trust. The sensor nodes in WSNs usually collaborate and communicate with neighbour nodes to perform their tasks. Therefore, the communication behaviour is always checked to evaluate whether the sensor node is normal or not. The unsuccessful communication maybe caused by malicious nodes or unstable communication channel. Therefore, just evaluating the communication behaviours is not enough for trust evaluation. In addition, it is generally known that all communications in WSNs will consume a certain amount of energy to transmit some data packets.

C. Calculation of the Communication Trust and Energy Trust

The information on a sensor node's prior behaviour is one of the most important aspects of the communication trust. However, communication channels between two sensor nodes are unstable and noisy, thus monitoring sensor node's behaviours in WSNs based on previous communication behaviours involves considerable uncertainty. Energy is an important metric in WSNs since sensor nodes are extremely dependent on the amount of energy they have. Malicious nodes always consume abnormal energy to launch malicious attacks.

Therefore, we use energy as a QoS trust metric to measure if a sensor node is selfish or maliciously exhaust additional energy. Using an energy prediction model, sensor nodes' energy consumption in different periods can be obtained. If the environment conditions do not change much, the energy consumption rate of normal nodes can maintain a stable value.

First, an energy threshold u is defined. When the residual energy Eres of one sensor node falls below the threshold value, the sensor node is not competent enough to perform its intended function. Thus, the energy trust of the sensor node is considered to be 0. Otherwise, the energy trust is calculated based on the energy consumption rate pene. The higher the energy consumption rate pene is, the less residual energy remains, which ultimately leads to a smaller ability of sensor nodes to complete the task. Thus, the trust values of the sensor nodes are considered to be smaller.

D. Calculation of the Data Trust

The trust of the data affects the trust of the network nodes that created and manipulated the data, and vice-versa, we introduce the evaluation of data trust in this section. The data packets have spatial correlation, that is, the packets sent among neighbour nodes are always similar in the same area. The data value of these packets in general follows some certain distribution, such as a normal distribution. For the sake of simplicity, in this paper, we also model the distribution of the data as a normal distribution.

E. Calculation of the Recommendation Trust

The recommendation trust is a special type of direct trust. When there are no direct communication behaviours between subject and object nodes, the recommendations from recommender are always taken into account for trust calculation. However, in most existing related works, the true and false recommendations are not distinguished. How to detect and get rid of false recommendations is important since it has great impact on the trust calculation.

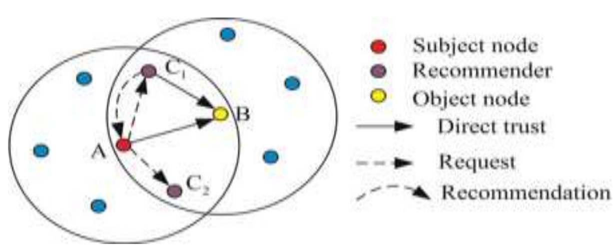

Figure 3: Calculation of the recommendation trust.

V. CONCLUSION

The severe constraints and demanding deployment environments of wireless sensor networks make computer security for these systems more challenging than for conventional networks. Limited power and resources of sensor nodes make the key challenge in maximizing lifetime as well as providing security in sensor networks. However, several properties of sensor networks may help address the challenge of building secure networks. The trust model has become important for malicious nodes detection in WSNs. It can assist in many applications such as secure routing, secure data aggregation, and trusted key exchange. Due to the wireless features of WSNs, it needs a distributed trust model without any central node, where neighbor nodes can monitor each other. In addition, an efficient trust model is required to handle trust related information in a secure and reliable way.

REFERENCES

1. N. Aboudagga, M.T. Refaei, M. Eltoweissy, L. DaSilva and J. Quisquater, “Authentication Protocols for Ad Hoc Networks : Taxonomy and Research Issues,” In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Quebec, Canada, 2005, pp. 96-104.
2. W. Du, R. Wang and P. Ning, “An Efficient Scheme for Authentication Public Keys in Sensor Networks,” In Proceeding of 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), IL, USA, 2005, pp. 58-67.
3. H. Cam, S. Ozdemir, D. Muthuavinashiappan and P. Nair, “Energy Efficient Security Protocol for Wireless Sensor Networks,” Vehicular Technology Conference, 2003, vol. 5, pp. 2981-2984.
4. C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, 2003.
5. J. P. Walters, Z. Liang, W. Shi and V. Chaudhary, “Wireless Sensor Network Security :ASurvey”,www.cs.wayne.edu/~weisong/papers/walters05-wsn-security-survey. pdf, 2005.
6. K.S.J. Pister, J.M. Kahn and B.E. Boser, “Smart Dust : Wireless networks of milli-meter scale sensor nodes”, 1999.

A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, “SPINS: Security protocols for sensor networks”, Wireless Networks, 2002, vol. 8, pp. 521-534.

7. H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, “Self-Securing Ad Hoc Wireless Networks.” In Seventh IEEE Symposium on Computers and Communications (ISCC '02), 2002.

8. D. Park, C. Boyd, E. Dawson. “Classification of Authentication Protocols: A Practical Approach.” Proceedings of the Third International Workshop on Information Security.
9. S. Zhu, S. Setia and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks.” In 10th ACM Conference on Computer and Communications Security (CCS '03).