International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M20-072014

AN EMPIRICAL REVIEW ON ALGORITHMIC APPROACHES FOR SECURITY ENHANCEMENT IN THE WIRELESS SENSOR NETWORKS

Sandeep Kaur
Department of Electronics and Communications Engineering
Rayat Institute of Engineering and Information Technology
Railmajra, Punjab, India

Vishal Walia
Department of Electronics and Communications Engineering
Rayat Institute of Engineering and Information Technology
Railmajra, Punjab, India

Dr. Rahul Malhotra
Professor
CTITR, Jallandhar
Punjab
India

ABSTRACT

A typical Wireless Sensor Network (WSN) consists of a sink node sometimes referred to as a Base Station and a number of small wireless sensor nodes. The base station is assumed to be secure with unlimited available energy while the sensor nodes are assumed to be unsecured with limited available energy. The sensor nodes monitor a geographical area and collect sensory information. Sensory information is communicated to the Base Station through Wireless hop by hop transmissions. Advances in electronics and wireless communication technologies have enabled the development of large-scale wireless sensor networks (WSNs). There are huge applications for wireless sensor networks, and security is vital for many of them. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the lack of infrastructure, which impose unique security challenges and make innovative approaches desirable. In this paper we present a survey of security issues in WSNs, address the state of the art in research on sensor network security, and present some future directions for research.

Keywords – Wireless Sensor Networks, Security, Integrity, Privacy, Confidentiality

INTRODUCTION

Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, autonomous, low-power, low-cost, small-size devices using sensors to cooperatively collect information through classical network infrastructure less ad-hoc wireless network. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of its unique characteristics. First, sensor nodes are very sensitive of production cost since sensor networks consist of a large number of sensor nodes. Akyildiz et al. presented that the cost of a sensor node should be much less than one dollar in order for sensor networks to be feasible. Therefore, most sensor nodes are resource restrained in terms of energy, memory, computation, and communication capabilities. Normally sensor nodes are powered by batteries, and recharging batteries are infeasible in many circumstances. Energy consumption becomes a key consideration for most sensor network protocols. Second, Sensor nodes may be deployed in public hostile locations, which make sensor nodes vulnerable to physical attacks by adversaries. Generally, adversaries are assumed to be able to undetectably take control of a sensor node and extract all secret data in the node. Furthermore, the scale of sensor networks is considerably large, and the network topology is dynamically adjusted, because some nodes may die out of running out of energy or failure, and new nodes may join the network to maintain desirable functionality. Two main security challenges in secure data aggregation are confidentiality and integrity of data. While traditionally encryption is used to provide end to end confidentiality in Wireless Sensor Network (WSN), the aggregators in a secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data. Thus, while data aggregation improves energy efficiency of a network, it complicates the existing security challenges.

In the classical and most of the network attacks, the assailant injects enormous amount of junk packets into the network which leads to the thrashing of network resources and causes congestion among the wireless networks. The prevention mechanism divides into two categories - Local and Global. In the scenario of local solution, the protection of individual nodes involves three categories - local solutions, changing IPs and creating client bottle neck. By installing the filter on the local router to detect the infiltrating IP packets is stopped using time worn short term solutions. By changing the victims IP address is one of the techniques to prevent the attacker from accessing its network, however this technique is not effective, many attacker node will easily identify the newer IP address. The major objective behind this technique is creating bottleneck process on the zombie computers, for example making simple puzzle to solve before establishing connection or a software already installed in host computer asks to answer random question whenever attacker computer try to establish connection.

The local solution consumes some time to perform connection this is unacceptable drawback. Global solutions are meant for changing technology, there are three techniques to implement them including Improving entire internet security, Using global coordinate filters and Source IP address tracing. The classical technique is to prevent attacking nodes by collecting its time. If this filters are installed in internet, a host can send information about the attacker node that it has detected to the filter, the filter will stop attacking packets along with their path. This is one of the effective methods to prevent malicious threat. The main objective of this approach is to trace the intruder’s path to the puzzle solving computers to stop their attack or to find the original attacker, and to take necessary action against it repeated attacks. However these techniques are not effective, because if the attacker node uses forged IP address, some of the hierarchical attacking structures hide the attacker from zombie computer. These are some major drawbacks. In the proposed scheme the fast forwarding and quick transferring problems are prevented by controlling the allocation vector, this technique increases Traffic on the network, Speed of data on nodes and Transmission time elapse. Cluster Head (CH) is also a wireless sensor node, which has more computational power comparing to all other sensor nodes. These cluster Heads are responsible for sharing all other sensor nodes information to the Base Station. The Base Station selects the Cluster head.

GOALS WITH SECURITY

Wireless sensor networks are vulnerable to many attacks because of broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environments where they are left unattended. Similar to other communication systems, WSNs have the following general security goals:

- Confidentiality: protecting secret information from unauthorized entities
- Integrity: ensuring message has not been altered by malicious nodes
- Data Origin Authentication: authenticating the source of message;
- Entity Authentication: authenticating the user/node/base-station is indeed the entity whom it claims to be
- Access control : restricting access to resources to privileged entities
- Availability: ensuring desired service may be available whenever required

SPECIFIC SECURITY OBJECTS WITH WSN

- Forward secrecy: preventing a node from decrypting any future secret messages after it leaves the network
- Backward secrecy: preventing a joining node from decrypting any previously transmitted secret message
- Survivability: providing a certain level of service in the presence of failures and/or attacks
- Freshness: ensuring that the data is recent and no adversary can replay old messages
- Scalability: supporting a great number of nodes
- Efficiency: storage, processing and communication limitations on sensor nodes must be considered

LITERATURE REVIEW AND RELATED EARLIER WORK

KEY DISTRIBUTION AND MANAGEMENT

Security of large scale densely deployed and infrastructure-less wireless networks of resource limited sensor nodes calls for efficient key distribution and management mechanisms. This is one of the most popular research fields in the secure sensor networks, and plenty of approaches are proposed.

STRAIGHTFORWARD APPROACHES

The simplest method of key distribution is to preload a single network-wide key into all nodes before deployment. Only one single key is stored in the nodes' memory and once deployed in the network, there is no need for a node to perform key discovery or key exchange since all the nodes in communication range can transfer messages using the key which they already share. On the other hand, this scheme suffers a severe drawback that compromise of a single node would cause compromise of the entire network through the shared key. Thus it fails in providing the basic secure requirement of a sensor network by making it easy for an adversary trying to attack. An alternative key distribution scheme is fully pairwise keys scheme, i.e., every node in the sensor network shares a distinct key with every other node in the network. The main problem with this pairwise key scheme is its poor scalability. The number of keys that must be stored in each node is proportional to the total number of nodes in the network. Since sensor nodes are resource-constrained, this brings significant overhead which limits the scheme's applicability except for it can only be effectively used in smaller networks. The method of Kerberos-like key distribution is popular in a lot of networks environment. In sensor networks, we can use a trusted, secure base station as an arbiter to provide link keys to sensor nodes. The sensor nodes authenticate themselves to the base station, after which the base station generates a link key and sends it to both parties securely. An example of such a protocol is SNEP, a part of the SPINS security infrastructure . However, this kind of schemes suffers high energy consumption, which makes it inapplicable in most of sensor network applications.

SCHEMES BASED ON INITIAL TRUST MODEL

In LEAP, Zhu, Setia, and Jajodia proposed a key distribution scheme based on initial trust mode. Every node shares a common master key K and a keyed one-way hash function H. Upon deployed, nodes begin to discover all neighbor nodes and establish pairwise key using K and H. For example, the pairwise key between node u and v can be HHK(u)(v) or HK(u||v). After establishing every pairwise key, all nodes eliminate the master key. LEAP assumes that T (the time necessary for an adversary to compromise a sensor node) is larger than the maximum time for nodes to complete the key distribution. If this assumption holds, LEAP is secure. However, sensors may be deployed in different phases, and new sensors need to be added when previously deployed sensors fail or when the capability of the existing network is turned to be insufficient. A major disadvantage of LEAP is not supporting multi-phase deployment—new nodes cannot create pairwise keys with previous nodes. Proposal in partially solves this problem by that there are many distinct master keys, each of which is for one phase. Every node u in phase i stores the master key Ki and all other HKj (u), where j > i. Every two adjacent nodes in same phase can establish pairwise key like LEAP. If node u in phase i and node v in phase j want to establish pairwise key, supposing i < j, they both can compute HHKj (u)(v) and get the pairwise key. Every node only eliminates its phase mater key, and keeps the rest. A drawback of this scheme steps up that an adversary who comprises one node can duplicate many nodes which can establish pairwise keys with later phase nodes. And the number of phases has to be determined prior to first deployment.

Another initial-trust-like scheme is addressed in , and is further enhanced in . They assume that adversaries can monitor only small portion of sensor nodes, due to randomly deployment of sensor networks. Initially, each pair of neighbor nodes only broadcast their pairwise key in plaintext. Afterwards, they can utilize multihop and multipath indirect secure links to exchange other secret data, which results in higher security.

BASIC RANDOM PROBABILISTIC KEY DISTRIBUTION SCHEME

Eschenauer and Gligor first proposed random key probabilistic distribution schemes (EG scheme) based on random graph theory . A random graph is a graph that is generated by starting with a set of n vertices and adding edges between them at random. In Erd¨os- R´enyi model, a random graph is denoted by G(n, p), in which every possible edge occurs independently with probability p. Erd¨os and R´enyi showed that, to achieve almost one hundred percent graph connectivity, every two vertices only need to have relatively lower probability P0 of existence of direct link. More than often, sensor node are randomly deployed and the number of nodes in a sensor network is massive. We may think of a wireless sensor network as a graph, nodes as vertices, and links as edges. Using random graph theory, we can theoretically analyze the connectivity of sensor networks and design WSN-specific security protocols. Since EG scheme, the random probabilistic approaches are gaining many attentions in secure wireless sensor networks, and many interesting protocols are proposed. Pietro et al. questioned the realistic assumption of random graph model in WSNs, and proposed another geometric random model for WSNs. Wu and Stinson further discussed these models and validated the use of the random graph model in computing the connectivity of WSNs. Nevertheless, random-graph-based analyses are still prevailing in protocols of WSNs.

ENHANCEMENT OF RANDOM KEY DISTRIBUTION

Chan, Perrig, and Song introduced two variations of EG Scheme, i.e., q-composite random key predistribution and multipath key reinforcement. The q-composite random key predistribution scheme requires that two nodes have at least q common keys to set up a link and use all common keys instead of first one to establish pairwise key. As the number of key overlap between two nodes increases, it becomes harder for an adversary to break their communication link. At the same time, to maintain the probability that two nodes establish a link with q common keys, it is necessary to reduce the size of the key pool, which poses a possible security breach in the network as the adversary now has to compromise only a few nodes to gain a large portion of key pool. Therefore the challenge of the q-composite scheme is to choose an optimal value for q while ensuring that security is not sacrificed. However, the optimal value 6 for q is strictly related to the number of nodes that adversaries may capture, which is dynamic and cannot be precisely determined while network parameters are designated. Therefore, the benefit of q-composite (q > 1) mode might be trivial. The multipath reinforcement scheme is similar to , using multipath indirect secure link to exchange secret data to offer good security with additional communication overhead, suitable for occasions where security is more of a concern than bandwidth or power drain.

GROUP KEY DISTRIBUTION

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

A Wireless Sensor Network (WSN) typically consists of a sink node sometimes referred to as a Base Station and a number of small wireless sensor nodes. The base station is assumed to be secure with integrity.

Wireless sensor networks are inherently collaborative environments in which sensor nodes often communicate in groups that typically are dynamic. Efficient group key management schemes are demanded for secure communications under this collaborative model. General speaking, many traditional binary-tree-based group key management schemes and broadcast approaches, such as logical key hierarchy, one-way function chain tree, and subset-cover broadcast encryption, can be adapted into wireless sensor networks. Currently many proposed group key management schemes in WSNs are based on exclusion basis systems (EBS), presented by Eltoweissy et al. , which is a combinatorial formulation of the group key management problem that produces optimal results with respect to the parameters n, k and m, where n is the size of the group, k is the number of keys stored by each member, and m is the exact number of re-key messages to exclude one member.

To propose and defend the research work, a number of research papers are analyzed. Following are the excerpts from the different research work performed by number of academicians and researchers :

Mitigating Sandwich Attacks against a Secure Key Management Scheme in Wireless Sensor Networks for PCS/SCADA Hani Alzaid and DongGook Park and Juan Gonz´alez Nieto and Ernest Foo April 28, 2010 : Alzaid et al. proposed a forward & backward secure key management scheme in wireless sensor networks for Process Control Systems (PCSs) or Supervisory Control and Data Acquisition (SCADA) systems. The scheme, however, is still vulnerable to an attack called the sandwich attack that can be launched when the adversary captures two sensor nodes at times t1 and t2, and then reveals all the group keys used between times t1 and t2. In this paper, a fix to the scheme is proposed in order to limit the vulnerable time duration to an arbitrarily chosen time span while keeping the forward and backward secrecy of the scheme untouched.

International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011 39 Cross Layer Security Framework for Wireless Sensor Networks Kalpana Sharma and M.K. Ghose. Department of CSE, SMIT, Sikkim : Since the data collected by the nodes of WSN are sensitive and vulnerable to attack, there's a need of making the Wireless Sensor Networks (WSN) immune to attacks. Most of the researchers have come up with security solution to WSN based on layered approach. Layered approach has noticeable flaws like 'redundant' security or 'inflexible' security solutions. In this paper a new security scheme is proposed based on the concept of cross layer design methodology. Outline on the existing cross layer security schemes are also presented. The proposed approach doesn't claim to be immune to all the security attacks but this new approach certainly gives a new direction towards WSN security.

Efficient weakly secure network coding scheme against node conspiracy attack based on network segmentation Rong Du1, Chenglin Zhao, Shenghong Li and Jian Li, 2014, In this paper, the authors consider the problem of building a secure network against node conspiracy attack that based on network segmentation. Network coding has demonstrated its great application prospects in wireless sensor network (WSN) transmission. At the same time, it is facing a variety of security threats, especially conspiracy attack. In existing research, secure coding design strategies are much more than secure topological structure. In this background, a weakly secure scheme is proposed from the perspective of topology and network segmentation. Based on the network segmentation and topology design, the network coding transmission is weakly secure. The authors conduct a simulation to show that the proposed scheme can efficiently prevent conspiracy attack. In this work, the authors have investigated the topology design and network segmentation issue for weakly secure against node conspiracy attack.

ATTACKS AND COUNTERMEASURES

SECURE ROUTING

Routing is a basic functionality of any network, there are various attacks and corresponding countermeasures for WSNs. Sybil attack and wormhole attack are two major routing attacks specifically for WSNs. Karlof and Wagner first considered routing security in wireless sensor networks systematically. They addressed security goals for routing in sensor networks, showed how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduced two classes of novel attacks against sensor networks — sinkholes and HELLO floods, and analyzed the security of all major sensor network routing protocols. Sink is an alias of base station in sensor networks. In a sinkhole attack, the adversary’s goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes along or near the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks. They also described crippling attacks against all of them and suggest countermeasures and design considerations.

SYBIL ATTACK

Sybil attack is a harmful threat to sensor networks, in which a malicious node illegally forges an unbounded number of identities. The Sybil attack can disrupt normal functioning of the sensor network, such as the multipath routing, used to explore the multiple disjoint paths between source-destination pairs. Douceur first presented the Sybil attack problem in the peer-to-peer distributed systems. He pointed out that it could defeat the redundancy mechanisms of the distributed storage systems. Newsome et al. analyzed the threat posed by the Sybil attack to wireless sensor networks. They established a classification of different types of the Sybil attack, proposed several techniques to defend against the Sybil attack, and analyzed their effectiveness quantitatively. Zhang et al. proposed a light-weight identity certificate method using to thwart Sybil attack. This method uses a two-level Merkle hash tree to create certificates. Each sensor node is pre-assigned a unique secret key to derive one-way key chains. An identity certificate is also distributed to each node, which associates the node's identity with its one-way key chain. To securely demonstrate its identity, a node first presents its identity certificate, and then proves that it possesses or matches the associated unique information. An extension of this method exploits node deployment knowledge to reduce the computational overhead at each node. However, the scalability problem of this method adversely affects its use in a large scale sensor network.

WORMHOLE ATTACK

Since sensors use a radio channel to send information, malicious nodes can eavesdrop the packets, tunnel them to another location in the network, and retransmit them. This generates a false scenario that the original sender is in the neighborhood of the remote location. The tunneling procedure forms a wormhole attack. Wang and Bhargava proposed a mechanism, MDS-VOW, to detect wormholes in a sensor network. MDS-VOW first reconstructs the layout of the sensors using multi-dimensional scaling. Then MDS-VOW detects the wormhole by visualizing the anomalies introduced by the attack. The anomalies, which are caused by the fake connections through the wormhole, bend the reconstructed surface to pull the sensors that are faraway to each other. Through detecting the bending feature, the wormhole is located and the fake connections are identified. Yun et al. proposed another countermeasure named WODEM against the wormhole attack. In WODEM, a few detector nodes equipped with location-aware devices and longer-lasting batteries detect wormholes, and normal sensor nodes are only required to forward control packets from the detector nodes. Then a pair of detectors can detect the wormhole attack between them.

DOS ATTACK

Denial of service (DoS) attack is a pervasive threat to most networks. Due to the characteristics of energy-sensitiveness and resource-limitedness, sensor networks are very vulnerable for DoS attack. Wood and Stankovic explored various DoS attacks that may happen in every network layers of sensor networks. Mihui, Inshil, and Kijoon proposed a DoS detection method via practical entropy estimation on hierarchical sensor networks reflecting resource constraints of sensors. In order to enhance the accuracy of detection even in the various deployments of attack agents, they deployed hierarchically entropy estimators according to network topology, and a main estimator synthesizes localized computation. This entropy estimator is simplified by only multiplication calculation instead of logarithm, in addition to providing higher estimation precision of entropy compared to the conventional entropy estimation.

NODE CLONE ATTACK

Sensor nodes deployed in hostile environments are vulnerable to capture and compromise. An adversary may extract secret information from these sensors, clone and intelligently deploy them in the network to launch a variety of insider attacks. Chan and Perrig catalog a number of attacks that can be made using replicated nodes

GENERAL INTRUSION DETECTION AND INTRUSION TOLERANCE

Agah et al. proposed an intrusion detection framework of sensor networks using game theory. They applied three different schemes for defense. The main concern in all three schemes is finding the most vulnerable node in a sensor network and protecting it. In the first scheme they formulated attack-defense problem as a two-player, nonzero-sum, non-cooperative game between an attacker and a sensor network. This game achieves Nash equilibrium and thus leading to a defense strategy for the network. In the second scheme they used Markov Decision Process to predict the most vulnerable senor node. In the third scheme they used an intuitive metric (node's traffic) and protected the node with the highest value of this metric. Based on the DESERT tool, which has been proposed for component-based software architectures, Inverardi, Mostarda, and Navarra derived a framework that permits to dynamically enforce a set of properties of the sensors behavior. This is accomplished by an IDS specification that is automatically translated into few lines of code installed in the sensors. This realizes a distributed system that locally detects violation of the sensors interactions policies and is able to minimize the information sent among sensors in order to discover attacks over the network.

CONCLUSION AND SCOPE OF FUTURE WORK

As WSN develop in provision zone and are utilized all the more much of the time, the need for security in them gets inexorable and key. Be that as it may, the characteristic qualities of WSN acquire demands to of sensor hubs, for example, constrained vitality, handling competence, and capacity limit, and so forth. These demands make WSN altogether different from conventional remote systems. Therefore, numerous creative security conventions and procedures have been produced to meet this test. In this paper, we diagram security and protection issues in sensor systems, address the state of the workmanship in sensor system security, and examine some future bearings for examination. As to the future work, the existing work might be enhanced regarding multilayered security to enhance the secrecy of WSN.

REFERENCES

[1] Efficient weakly secure network coding scheme against node conspiracy attack based on network segmentation Rong Du, Chenglin Zhao, Shenghong Li and Jian Li, 2014

[2] Energy Efficient Security For Wireless Sensor Networks by Abidalrahman Moh’d, 2013

[3] Energy Effieient Routing Protocols and Keying techniques etc. Security in cognitive wireless sensor networks. Challenges and open problems Alvaro Araujo, Javier Blesa, Elena Romero and Daniel Villanueva Araujo et al. EURASIP Journal on Wireless Communications and Networking 2012

[4] International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011 39 Cross Layer Security Framework for Wireless Sensor Networks Kalpana Sharma and M.K. Ghose. Department of CSE, SMIT, Sikkim

[5] Mitigating Sandwich Attacks against a Secure Key Management Scheme in Wireless Sensor Networks for PCS/SCADA Hani Alzaid and DongGook Park and Juan Gonz´alez Nieto and Ernest Foo April 28, 2010

[6] A Survey on Security in Wireless Sensor Networks, Zhijun Li and Guang Gong, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada