International Journal of Future Generation Communication and Networking
Vol. 9, No. 7 (2016), pp. 173-184
http://dx.doi.org/10.14257/ijfgcn.2016.9.7.17

Research on Security Mechanisms for Wireless Sensor Network

Chengwei Hu

Guangzhou Civil Aviation College, Guangzhou； China
31436138@qq.com

Abstract

The Internet of Things is a paradigm where everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will allow them to communicate with one another and with other devices and services over the Internet to accomplish some objective. Wireless Sensor Networks (WSN) is one such technology that connects the virtual world and the physical world where nodes can autonomously communicate among each other and with intelligent systems. In our paper we mainly focus on the security threats in WSN. We have presented the summery of the WSNs threats affecting different layers along with their defense mechanism.

Keywords*: WSN, protocol stack, architecture, attack, defense mechanism*

1. Introduction

With the development of embedded system and network technology, there has been growing interest in providing fine-grained metering and controlling of living environments using low power devices. Wireless Sensor Networks (WSNs), which consist of spatially distributed self-configurable sensors, perfectly meet the requirement. The sensors provide the ability to monitor physical or environmental conditions, such as temperature, humidity, vibration, pressure, sound, motion and *etc*, with very low energy consumption.

The sensors also have the ability to transmit and forward sensing data to the base station. Most modern WSNs are bi-directional, enabling two-way communication, which could collect sensing data from sensors to the base station as well as disseminate commands from base station to end sensors. The development of WSNs was motivated by military applications such as battlefield surveillance; WSNs are widely used in industrial environments, residential environments and wildlife environments. Structure health monitoring, healthcare applications, home automation, and animal tracking become representative WSNs applications.

2. Wireless Sensor Network Architecture

A typical Wireless Sensor Network (WSN) is built of several hundreds or even thousands of "sensor nodes". The topology of WSNs can vary among star network, tree network, and mesh network. [1] Each node has the ability to communication with every other node wirelessly, thus a typical sensor node has several components: a radio transceiver with an antenna which has the ability to send or receive packets, a microcontroller which could process the data and schedule relative tasks, several kinds of sensors sensing the environment data, and batteries providing energy supply. [2]

ISSN: 2233-7857 IJFGCN

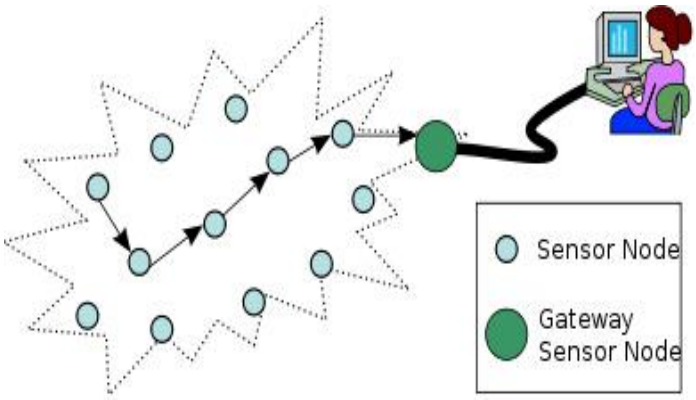

Figure 1. Typical Multi-hop Wireless Sensor Network Architecture

Sensor networks are expected to play an essential role in the upcoming age of pervasive computing. Due to their constraints in computation, memory, and power resources, their susceptibility to physical capture, and use of wireless communications, security is a challenge in these networks. Current research on sensor networks is mostly built on a trusted environment. Several exciting research challenges remain before we can trust sensor networks to take over important missions [3].

3. Sensor Deployment and Coverage

In a typical sensor network application, sensors are to be placed (or deployed) so as to monitor a region or a set of points. In some applications we may be able to select the sites where sensors are placed while in others (*e.g.*, in hostile environments) we may simply scatter (*e.g.*, air drop) a sufficiently large number of sensors over the monitoring region with the expectation that the sensors that survive the air drop will be able to adequately monitor the target region. When site selection is possible, we use deterministic sensor deployment and when site selection isn’t possible, the deployment is nondeterministic. In both cases, it often is desirable that the deployed collection of sensors be able to communicate with one another, either directly or indirectly via multihop communication. So, in addition to covering the region or set of points to be sensed, we often require the deployed collection of sensors to form a connected network. For a given placement of sensors, it is easy to check whether the collection covers the target region or point set and also whether the collection is connected. For the coverage property, we need to know the sensing range of individual sensors (we assume that a sensor can sense events that occur within a distance r, where r is the sensor’s sensing range, from it) and for the connected property, we need to know the communication range, c, of a sensor. We have established the following necessary and sufficient condition for coverage to imply connectivity.

Theorem 1
When the sensor density (*i.e.*, number of sensors per unit area) is finite, $c \geqslant 2r$ is a necessary and sufficient condition for coverage to imply connectivity.

Theorem 2
When $c \geqslant 2r$, k-coverage of a convex region implies k-connectivity. Notice that k-coverage with $k > 1$ affords some degree of fault tolerance, we are able to monitor all points so long as no more than $k - 1$ sensors fail. Huang and Tseng [25] develop algorithms to verify whether a sensor deployment provides k-coverage. Other variations of the sensor deployment problem also are possible. For example, we may have no need for sensors to communicate with one another. Instead, each sensor communicates directly with a base station that is situated within the communication range. of all sensors. In

another variant [23, 24], the sensors are mobile and self deploy. A collection of mobile sensors may be placed into an unknown and potentially hazardous environment. Following this initial placement, the sensors relocate so as to obtain maximum coverage of the unknown environment. They Step 1: [Achieve Coverage]

Let $\delta = (\frac{\sqrt{3}}{2} + 1)r$. Place a sensor at (i, j δ), i even and j integer as well as one at (i + r/2, j δ), I odd and j integer.

Step 2: [Achieve Connectivity]

Let $\beta = \frac{\sqrt{3}}{2}r$. Place a sensor at (0, j $\delta \pm \beta$), j odd

Communicate the information they gather to a base station outside of the environment being sensed. A distributed potential-field-based algorithm to self deploy mobile sensors under the stated assumptions is developed and a greedy and incremental self-deployment algorithm I developed in [23]. A virtual-force algorithm to redeploy sensors so as to maximize coverage also is developed by Zou and Chakrabarty [17]. Poduri and Sukhatme [18] develop a distributed self-deployment algorithm that is based on artificial potential fields and which maximizes coverage while ensuring that each sensor has at least k other sensors within its communication range.

4. Wireless Sensor Network Protocol Stack

The sensor nodes are usually scattered in a sensor field. The protocol stack used by all sensor nodes is given in Fig. 2. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. The protocol stack consists of the application layer, transport layer, network layer, data link layer, physical layer, power management plane, mobility management plane, and task management plane. Depending on the sensing tasks, different types of application software can be built and used on the application layer. The transport layer helps to maintain the flow of data if the sensor networks application requires it. The network layer takes care of routing the data supplied by the transport layer. Since the environment is noisy and sensor nodes can be mobile, the MAC protocol must be power aware and able to minimize collision with neighbors' broadcast. The physical layer addresses the needs of a simple but robust modulation, transmission and receiving techniques. In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes coordinate the sensing task and lower the overall power consumption. [5]

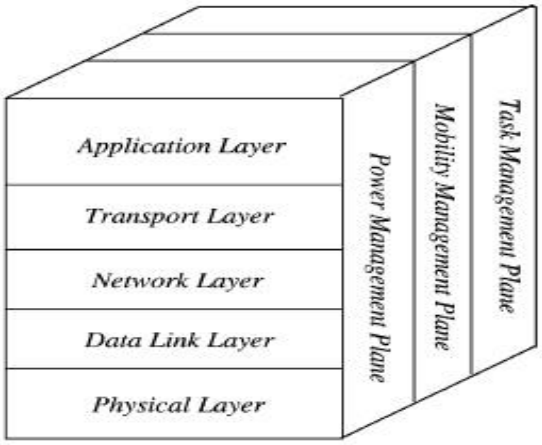

Figure 2. The Sensor Networks Protocol Stack

The power management plane manages how a sensor node uses its power. For example, the sensor node may turn off its receiver after receiving a message from one of its neighbors. This is to avoid getting duplicated messages. Also, when the power level of the sensor node is low, the sensor node broadcasts to its neighbors that it is low in power and cannot participate in routing messages. The remaining power is reserved for sensing. The mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who are their neighbor sensor nodes. By knowing who the neighbor sensor nodes are, the sensor nodes can balance their power and task usage. The task management plane balances and schedules the sensing tasks given to a specific region. Not all sensor nodes in that region are required to perform the sensing task at the same time. As a result, some sensor nodes perform the task more than the others depending on their power level. These management planes are needed, so that sensor nodes can work together in a power efficient way, route data in a mobile sensor network, and share resources between sensor nodes. Without them, each sensor node will just work individually. From the whole sensor network standpoint, it is more efficient if sensor nodes can collaborate with each other, so the lifetime of the sensor networks can be prolonged.

5. Wireless Sensor Network Routing

Traditional routing algorithms for sensor networks are data centric in nature. Given the unattended and untethered nature of sensor networks, data centric routing must be collaborative as well as energy- conserving for individual sensors. Kannan et al. [19, 20] have developed a novel sensor-centric paradigm for network routing using game-theory. In this sensor-centric paradigm, the sensors collaborate to achieve common network-wide goals such as route reliability and path length while minimizing individual costs. The sensor-centric model can be used to define the quality of routing paths in the network (also called path weakness). Kannan et al. [20] describe inapproximability results on obtaining paths with bounded weakness along with some heuristics for obtaining strong paths. The development of efficient distributed algorithms for approximately optimal strong routing is an open issue that can be explored further.

Energy conservation is an overriding concern in the development of any routing algorithm for wireless sensor networks. This is because such networks are often located such that it is difficult, if not impossible, to replenish the energy supply of a sensor. Three forms – unicast, broadcast and multicast – of the routing problem have received significant attention in the literature. The overall objective of these algorithms is to either maximize the lifetime (earliest time at which a communication fails) or the capacity of the network (amount of data traffic carried by the network over some fixed period of time). Assume that the wireless network is represented as a weighted directed graph G that has n ver-tices/nodes and e edges. Each node of G represents a node of the wireless network. The weight w(i, j) of the directed edge (i, j) is the amount of energy needed by node i to transmit a unit message to node j.In the most common model used for power attenuation, signal power attenuates at the rate a/rd, where a is a media dependent constant, r is the distance from the signal source, and d is another constant between 2 and 4 [48]. So, for this model, w(i, j) = w(j, i) = c ∗ r(i, j)d, where r(i, j) is the Euclidean distance between nodes i and j and c is a constant. In practice, however, this nice relationship between w(i, j) and r(i, j) may not apply. This may, for example, be due to obstructions between the nodes that may cause the attenuation to be larger than predicted. Also, the transmission properties of the media may be asymmetric resulting in.

$$w(i,j) \neq w(j,i).$$

6. Security Architecture and Requirements of Wireless Sensor Network

Depending on the application, a sensor network must support certain QoS (guaranteed delivery [9]) aspects such as real-time constraints (*e.g.*, a physical event must be reported within a certain period of time), robustness (*i.e.*, the network should remain operational even if certain well defined failures occur), tamper-resistance (*i.e.*, the network should remain operational even when subject to deliberate attacks), eavesdropping resistance (*i.e.*, external entities cannot eavesdrop on data traffic), and unobtrusiveness or stealth (*i.e.*, the presence of the network must be hard to detect). These requirements may impact other dimensions of the design space such as coverage and resources [6]. Current security mechanisms in ad-hoc sensor networks do not guarantee reliable and robust network functionality. Even with these mechanisms, the sensor nodes could be made non-operational by malicious attackers or physical break-down of the infrastructure. Measurement of the network characteristics in a 'threat' of network failure is essential to understand the behavior of these networks. The security architecture (security map) of security issues in WSN is drawn as in the following figure:

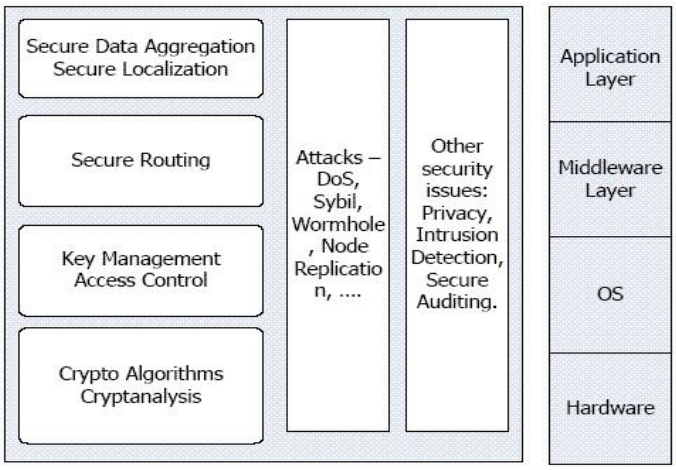

Figure 3. Security Architecture for WSN

The security requirements [9] of a wireless sensor network can be classified as follows:

Authentication:
As WSN communicates sensitive data which helps in many important decisions making. The receiver needs to ensure that the data used in any decision-making process originates from the correct source. Similarly, authentication is necessary during exchange of control information in the network.

Integrity:
Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident.

Data Confidentiality:
Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.

Data Freshness:
Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To ensure that no old messages replayed a time stamp can be added to the packet.

Availability:
Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network.

Self-Organization:
A wireless sensor network believes that every sensor node is independent and flexible enough to be self-organizing and self-healing according to different hassle environments. Due to random deployment of nodes no fixed infrastructure is available for WSN network management. Distributed sensor networks must self-organize to support multihop routing.

Time Synchronization:
Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off periodically.

Secure Localization:
The sensor network often needs location information accurately and automatically. However, an attacker can easily manipulate nonsecured location information by reporting false signal strengths and replaying signals, *etc*.

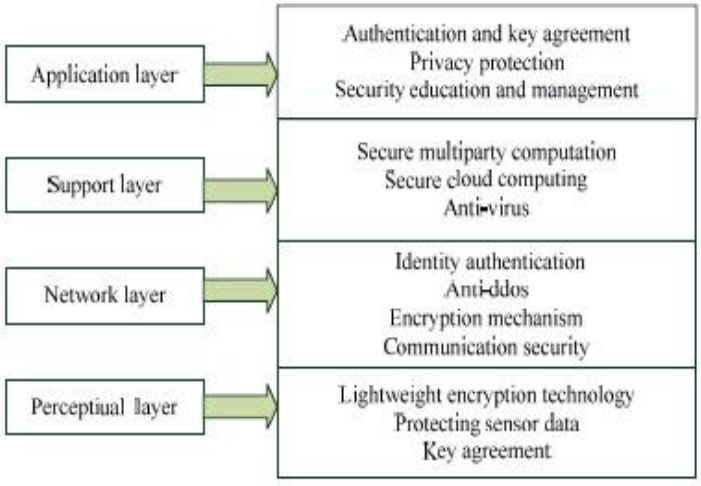

Figure 4. Security Requirements in WSNs Classification

7. Types of Attacks on Wireless Sensor Network

Wireless sensor networks are at risk for security attacks due to their broadcast nature of the transmission medium. Moreover, wireless sensor networks have an extra exposure because of nodes are often placed in a hostile (or unsafe) environment where they are not actually safe. The foremost attacks are: Denial of Service, Sybil attack, Wormhole attack, Selective Forwarding attack, Sinkhole attack, Passive information gathering, Hello flood attack, Node capturing, false or malicious node, *etc*.

Denial of Service
It occurs when involuntary failure or malicious node occurs. The merest Denial of Service attack tries to beat the resources available to the victim node, by sending additional unnecessary packets and thus prevents logical network users from accessing resources to which they are allowed [9]. There are several types of DoS attacks that might be performed in WSN in different layers. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de synchronization.

The Sybil attack
In this attack, a single node presents multiple identities to other nodes in network and will send incorrect information to a node in the network. The incorrect information can be a mixture of affairs, such as position of nodes, signal strengths, and comprising nodes that do not exist. Some preventive techniques like Authentication and encryption techniques will not allow an outsider to launch a Sybil attack on the sensor network. On the other hand, an insider cannot be disallowed in the network from participating, but it can only be done by using the identities of the nodes that it has compromised. But we can prevent such an insider attack by using Public key cryptography, which will be too expensive for using in these types of resource constrained sensor networks.

The Wormhole attack
Node (sender node) in the network broadcasts a message to the other node (receiver node) in the network, further the receiving node attempts to broadcast the message to its neighbors. It thinks that the message was sent from the sender node(where as it is normally out of range), so they try to send the message to the starting node, simply it never arrives to starting node because it is too far away from the current node . Wormhole attack is a substantial threat to wireless sensor networks, since, this type of attack does not compel compromising a sensor in the network instead, and the sensors start to discover neighboring information even at the initial phase. These attacks are very hard to contradict because routing information rendered by a node is unmanageable to verify.

Selective Forwarding attack
A selective forwarding attack site is typically most effective when the attacker is explicitly admitted on to data flow path. It is when certain nodes fail to forward many of the messages they receive.

Sinkhole attacks
Aim of this sort of attack is to lure almost all the traffic from a particular area through a compromised node, and makes that node look attractive to adjacent nodes with respect to the routing algorithm. These attacks are very hard to contradict because routing information rendered by a node is unmanageable to verify.

Passive Information Gathering
In this passive information gathering an intruder can easily pluck the data stream provided if he has parameters such as an suitably powerful receiver and well designed antenna. The physical locations of sensor nodes admits an attacker to locate the nodes and destroy them [3] since messages snaps the location of node and can detect specific message IDs and also other fields.

Hello flood attacks
These types of attacks can be induced by a node when it broadcasts a Hello packet with very high power, such that in the network a large number of nodes even far away choose

it as the parent. Now all messages needed to be routed multi-hop to the parent, thus increases delay.

False or Malicious Node
In wireless sensor networks almost of all attacks against security are caused by the insertion of imitation data by the compromise nodes within the network.

Node Capturing
Information stored on a particular sensor node that was captured, might be obtained by an adversary [13].

8. Defensive Mechanisms for Wireless Sensor Network

Here we highlights some of the preventive measures for all the attacks that are mentioned

DOS prevention
Preventing DoS attacks admit payment for network resources, force back, strong authentication and identification of traffic [1]. The technique applies authentication streams to secure the reprogramming process. which divides a program binary into a sequence of messages, each of which contains a hash of the adjacent message. [13]This mechanism ensures that a trespasser cannot pirate an ongoing program transmission; even it knows the hashing mechanism. This is because it would be virtually impossible to construct a message that matches the hash contained in the premature message.

Wormhole attack prevention
To prevent the wormhole attack admit, DAWWSEN routing protocol ,which is a proactive routing protocol based on the building of a hierarchical tree where the base station will be the root node, and the sensor nodes will be the leaf nodes of the tree. A great advantage of DAWWSEN is that it doesn’t compel any geographical data about the sensor nodes, and also doesn't acquire the time stamp of the packet as an approach for detecting a wormhole attack, which is most significant for the resource constrained nature of the sensor nodes.

Sybil prevention
Prevention against Sybil attacks are to employ identity certificates. The basic idea is very straightforward. Before deployment, setup the server, in such way that it assigns each sensor node with some inimitable information. Then the server will creates an identity certificate for binding this nodes identity to the assigned inimitable information, and downloads this information into the node. To securely certify its identity, a node must present its identity certificate, and then proves that it matches the associated inimitable information. For this it requires the exchange of several messages.

Passive information gathering prevention
Well-built encryption techniques need to be used to down play the threats of passive information gathering.

Node capture prevention
This issue can be solved by Localized Encryption and Authentication protocol (LEAP). LEAP is an efficient protocol for inter-node traffic authentication. And this protocol relies on a key sharing approach which authorizes in-network processing, and at the same time mitigates a number of possible attacks.

False or Malicious Node prevention
This attack basically should be checked in the Routing layer itself.

Hello flood attacks prevention
This can be avoided by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop. The table-2 contains the summary of the various attacks of WSN and also in short summarizes the defense mechanism.

Selective Forwarding attack prevention
To prevent against selective forwarding attacks a Multipath routing can be used . Messages routed over these paths are completely protected and the nodes are completely disjoint against selective forwarding attacks . And allows nodes to dynamically choose a packets next hop probabilistically from a set of possible prospects can further trim down the chances of an adversary gaining complete control of a data flow [14].

Sinkhole attacks prevention
Such attacks are very difficult to defend against. Geographic routing protocols that resistant to these type of attacks. Geographic routing protocols build up a topology on requirement using only localized connections, information and without initiation from the base station.

Table 1. WSNs Threats in Layers & Defense Mechanisms

ATTACKS	LAYERS INVOLVED	DEFENSES
DENIAL OF SERVICE	Physical, Link, Network Transport layers	Priority messages, hiding, monitoring, authorization, redundancy, Encryption
WORMHOLE	Link layer, Network layer	Dawwsen proactive routing protocol suspicious node detection by signal strength
SYBIL	Network layer, Application layer	Identity certificates
HELLO FLOOD	Network layer	Suspicious node detection by signal strength
SINK HOLE	Link layer, Network layer	Detection on MintRoute

9. Conclusions

All of the previously mentioned security threats, the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, serve one common purpose that is to compromise the integrity of the network they attack. Also In the past, focus has not been on the security of WSNs, but with the various threats arising and the importance of data confidentiality, security has become a major issue. Although some solutions have already been proposed, there is no single solution to protect against every threat. In our paper we mainly focus on the security threats in WSN. We have presented the summery of the WSNs threats affecting different layers along with their defense mechanism. We conclude that the defense mechanism presented just gives guidelines about the WSN security threats; the exact solution depends on the type of application the WSN is deployed for. There are many security mechanisms which are used in layer-by-layer basis as a security tool. [15]

References

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks", IEEE, Communications Magazine, vol. 40, no. 8, **(2013)**, pp. 102–105.
[2] S. Özdemir, "Secure data aggregation in wireless sensor networks via homomorphic encryption", Journal of the Faculty of Engineering and Architecture of Gazi University, vol. 23, no. 2, **(2010)**, pp. 365–373.
[3] C. Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges", Proceedings of the IEEE, vol. 91, no. 8, **(2013)**, pp. 1247–1256.
[4] M. Çakiroğlu and A. T. Özcerit, "Denial of service attack resistant MAC protocol design for wireless sensor networks", Journal of the Faculty of Engineering and Architecture of Gazi University, vol. 22, no. 4, **(2007)**, pp. 697–707, **2007**.
[5] T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: a survey", Journal of Information Assurance and Security, vol. 5, **(2013)**, pp. 31–44.
[6] H. Chan and A. Perrig, "Security and privacy in sensor networks", Computer, vol. 36, no. 10, pp. 103–105, 2003.
[7] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, vol. 35, **(2012)**, pp. 54-62.
[8] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Sensor Network Protocols and Applications (SNPA'03), **(2011)**.
[9] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks", IEEE Symposium on Security and Privacy (SP), **(2003)**.
[10] G. Jolly, M. C. Kuscu, P. Kokate and M. Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks", IEEE Symposium on Computers and Communications (ISCC'03), **(2014)**.
[11] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller and M. Sichitiu, "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes", WSNA'03, **(2003)**.
[12] K. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks", WSNA'03, **(2003)**.
[13] Y. C. Hu, A. Perrig and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", WiSe'03, **(2013)**.
[14] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks.WiSe'03, **(2013)**.
[15] R. D. Pietro, L. V. Mancini, Y. W. Law, S. Etalle and P. Havinga, "LKHW: A Directed Diffusion-Based Secure Multicast Scheme for Wireless Sensor Networks", 2013 International Conference on Parallel Processing Workshops (ICPPW'03), **(2013)**.
[16] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", CCS'03, **(2010)**.
[17] Y. Zou and K. Chakrabarty, "Sensor deployment and target localization in distributed sensor net-works, ACM Transactions on Embedded Computing Systems", vol. 3, no. 1, **(2004)**, pp. 61-91.
[18] S. Poduri and G. Sukhatme, "Constrained coverage for mobile sensor networks", IEEE Intl. Conf. on Robotics and Automation (ICRA'04), **(2004)**, pp. 165-171.
[19] R. Kannan, S. Sarangi, S. S. Iyengar and L. Ray, "Sensor-centric quality of routing in sensor networks", INFOCOM, **(2003)**.
[20] R. Kannan, S. Sarangi, S. Ray and S. Iyengar, "Minimal sensor integrity: Computing the vulnerability of sensor grids", Info. Proc. Letters, vol. 86, no. 1, **(2003)**, pp. 49-55.
[21] R. Kannan and S. S. Iyengar, "Game-theoretic models for reliable, path-length and energy-constrained routing in wireless sensor networks", IEEE Journal on Selected Areas in Communications, **(2004)**.
[22] S. Singh, M. Woo and C. Raghavendra, "Power-aware routing in mobile ad hoc networks", ACM/IEEE MOBICOM, **(2010)**.
[23] S. Slijepcevic and M. Potkonjak, "Power efficient optimization of wireless sensor networks", IEEE Intl. Conf. on Communications, **(2011).**
[24] A. Spyropoulos and C. Raghavendra, "Energy efficient communications in ad hoc networks using directional antenna", IEEE INFOCOM, **(2012)**.
[25] I. Stojmenovic, and Xu Lin, "Power-aware localized routing in wireless networks", IEEE Transactions on Parallel and Distributed Systems, **(2010)**.
[26] R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring and D. Estrin, "Habitat moni-toring with sensor networks", CACM, vol. 47, no. 6, **(2014)**, pp. 34-40.

Author

Chengwei Hu, he is a network and electronic communication expert, associate professor of electronic communication engineering, Responsible for the teaching management, laboratory construction, computer network teaching and study work in Guangzhou civil aviation college. His current research topics include Wireless Sensor Network, Cloud Computing and MIMO-OFDM technology.