Review of Key Management Mechanisms in Wireless Sensor Networks

SUN Dong-Mei[1] HE Bing[2]

[1](*Institute of Information Science, Beijing Jiaotong University, Beijing* 100044)

[2](*Electrical & Computer Engineering and Computer Science Department,*
University of Cincinnati, USA)

(E-mail: dmsun@center.njtu.edu.cn, heb@ececs.uc.edu)

Abstract Recent advancements in wireless communication and microchip techniques have accelerated the development of wireless sensor networks (WSN). Key management in WSN is a critical and challenging problem because of the inner characteristics of sensor networks: deployed in hostile environments, limited resource and *ad hoc* nature. This paper investigates the constraints and special requirements of key management in sensor network environment, and some basic evaluation metrics are introduced. The key pre-distribution scheme is thought as the most suitable solution for key management problem in wireless sensor networks. It can be classified into four classes: pure probabilistic key pre-distribution, polynomial-based, Blom′s matrix-based, and deterministic key pre-distribution schemes. In each class of methods, the related research papers are discussed based on the basic evaluation metrics. Finally, the possible research directions in key management are discussed.

Key words Key management, key pre-distribution, wireless sensor networks

1 Introduction

Recent advancements in wireless communications and micro electromechanical systems technologies have promoted the development and application of wireless sensor networks. A wireless sensor network is composed of large number of tiny sensor nodes, which are powered by batteries, equipped with sensing, data processing and short-range radio communications components[1].

When the sensors are deployed in a hostile field for military use, the network is vulnerable to security attacks due to the broadcast nature of transmission in the open air medium. Also the sensor nodes can be physically captured or destroyed or impersonated[2]. So the security issue is a very important problem to WSN.

To provide security, encryption technologies are used to achieve secret communications. To encrypt the data, a prerequisite is the secret keys should be set up among communicating sensor nodes.

Key management is the process in which keys are created, stored, protected, transferred, used and destroyed[3]. Keying means the process of achieving keys agreement among sensor nodes by deriving common secret keys among communicating parties. Pair-wise keying involves two parties agreeing on a shared session key while group keying is that more than two parties to set up the communication key. Currently several keying schemes have been proposed. Generally, there are three kinds of protocols[4]: The arbitrated keying protocols, self-enforcing protocols and pre-distribution keying protocols. The arbitrated keying scheme relies on some trusted central point, which is vulnerable to single point failure, also the ad hoc attribute of WSN makes it difficult to set up a network-wise available central point. The self-enforcing scheme uses the asymmetric encryption cryptography, which is limited by the current computation abilities and energy resources of sensor network technologies. So we mainly consider applying the pre-distribution key management scheme, in which keys are loaded into sensor nodes before deployment.

The paper is organized as follows. In Section 2, we analyze the special requirements and constraints of wireless sensor networks security schemes, and based on that some popular evaluation metrics are introduced. In Section 3, four major pre-distribution key management schemes are examined and discussed. Section 4 presents some additional research requirements and possible future research directions. Some conclusions are given in Section 5.

2 Security requirements and evaluation metrics

The basic constraints of sensor networks are: limited power/energy, low transmission range, limited storage and working memory, and unattended operations[4]. So when evaluating the performance of key management schemes, the following metrics are often used.

Received November 21, 2005; in revised form March 1, 2006

1) Connectivity (local/global): local connectivity is the probability that two nodes in communication range (neighboring nodes) share at least one key, while the global connectivity refers to the ratio of the number of nodes to be able to communicate in the post-keys-setup graph to the size of the whole network.

2) Resilience to sensor nodes capture: whenever a sensor node is captured, the information it carries may be retrieved by the adversary. The fraction of total keys information exposed to adversary can be considered as the resilience.

3) Scalability: the possibility that new nodes might be added later.

4) Memory efficiency: the amount of keying information needs to be stored in each node.

There are two naive solutions to be considered. One is called the network-wide "master" key approach, in which every node in the whole network share one common key. This method is memory efficient, but with weak resilience because capture of any node compromises the whole network.

Another method is pair-wise key approach, in which each node carries $N-1$ different keys to communicate with all other nodes (supposing the network size is N). Precisely, to secure groups of up to G nodes in the network, $\sum_{g=2}^{G}\binom{N}{g}$ keys have to be generated and deployed so that each node holds $\sum_{g=1}^{G-1}\binom{N-1}{g}$ keys[3]. The resilience is perfect but it is extremely not memory efficient. Also it is with poor scalability that no node has the key of newly added nodes.

So both simple solutions are not suitable for practical use.

3 Key pre-distribution schemes

The main idea of key pre-distribution schemes is that each node is distributed with the secret keys or secret information before deployed into the sensing area. Generally, a key pre-distribution scheme contains three phases: key pre-distribution phase, shared-key discovery phase and path-key establishment phase. The details of implementation of key pre-distribution scheme are discussed in [5]. The current proposed key pre-distribution schemes mainly can be classified into four classes: pure probabilistic key pre-distribution schemes, polynomial-based key pre-distribution schemes, Blom′s matrix-based key pre-distribution schemes and deterministic key pre-distribution schemes.

3.1 Pure probabilistic key pre-distribution schemes

Eschenauer and Gligor proposed the probabilistic key pre-deployed scheme[6], which is called basic scheme by most papers. In this scheme, three phases are needed to set up the communication keys: key pre-distribution, shared-key discovery, and path-key establishment. In the key pre-distribution phase (Fig. 1), each sensor node carries k distinct keys, which are randomly chosen from a big key pool (with size $P, P >> k$).

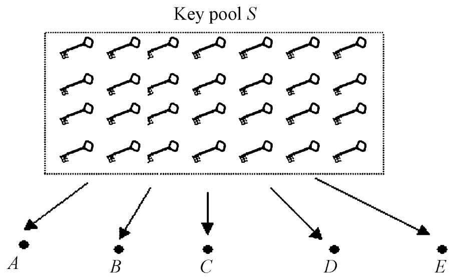

Fig. 1 Key pre-distribution phase

This set of k keys is called key ring and each key has a corresponding identifier.

The shared-key discovery phase happens when the sensor nodes are deployed into the sensed area. In the phase each node discovers its neighbors in radio range with which it shares common keys. In the end of shared-key discovery phase, links are set up between nodes that are not only in radio range but also sharing common keys. A sample topology is shown in Fig. 2. In this network, node pairs A and C, and B and C can set up secure links $\{A, C\}$, and $\{B, C\}$.

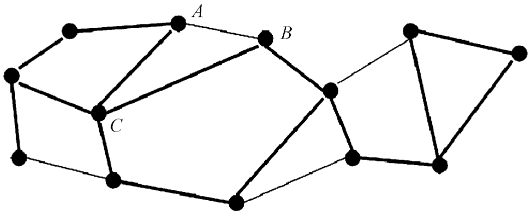

Fig. 2 Shared-key discovery and path-key establishment

For some node pairs in radio range but not to share a common key, they may be connected by two or more hop links in the path-key establishment phase. As shown in Fig. 2, nodes A and B are in communication radio range but do not share a common key. The path-key establishment phase assigns a path-key to the sensor nodes via node C and then they can set up secure link between them.

In this scheme, the random-graph theory[7] is used to design a key pre-distribution scheme. A random graph $G(n,p)$ is defined as a graph of n vertices, in which the probability that a link exists between two nodes is p. In the network graph two nodes are adjacent if they share a secret key. The graphic connectivity P_c has the relation with p as follows.

$$P_c = \lim_{n\to\infty} P_r[G(n,p) \ is \ connected] = e^{e^{-c}}$$

where $p = \dfrac{\ln(n)}{n} + \dfrac{c}{n}$, c is a real constant.

Given n we can find p and the expected degree of a node $d = p * (n-1)$ in which the resulting graph is connected with required probability P_c. Also the wireless connectivity constraints may limit neighborhoods to $n' << n$ nodes, then the probability of shareing a key between any two nodes in a neighborhood becomes

$$p' = \frac{d}{n'-1} >> p$$

This scheme works as below.

1) Choose c for a desired probability of connectivity P_c such that $P_c = e^{e^{-c}}$

2) Calculate p by $p = \dfrac{\ln(n)}{n} + \dfrac{c}{b}$, and

3) Determine the size of key pool P and the size of key ring k. P and k should satisfy[6]

$$1 - \frac{((P-k)!)^2}{(P-2k)!P!} \geqslant p$$

Thus, a key pool of size P is defined and each node can randomly select k keys in the key pool.

As we can see, most of the following key pre-distribution schemes are based on this model.

The crucial problem of this scheme is to choose P and k so that the probability of sharing at least one key between any two nodes is not less than the threshold probability p, which is calculated by the random graph theory. In this way the whole sensor network can achieve the predetermined connectivity probability P_c.

To improve the resilience to node capture, Chan *et al.*[8] proposed a modified version of the basic scheme. In this scheme, q common keys are needed to set up the common key with a hash function, rather than only one. By increasing the amount of key overlap required for key-setup, the resilience of the network against the node capture is increased. Actually, as the amount of required key overlap increases, it becomes exponentially harder for the adversary to attack. But because more shared keys are needed to set up a neighbor communication key, the local connectivity is decreased and the maximum support network size is limited.

In both schemes discussed above, many nodes share the same key. It is shown that averagely kn/P nodes share a common key in a network, where n nodes select k keys from a key pool with a size of P[8]. One node being captured will affect all the nodes that share the common key with it, even far from it. To remedy the key overlapping problem, Huang and Du[9] developed a node-based key pre-distribution scheme, in which different keys are used on different links. The primary idea is, for any node u, instead of selecting keys from the key pool, it selects $t = \left[\frac{d}{2}\right]$ different nodes from the $n-1$ nodes and pre-distributes symmetric keys between the node u and the t node set. In this node-based scheme, no two links being established use the same keys. And the resilience against node capture is improved as each captured node only affects those nodes sharing a link with it.

All the previous schemes do not consider the deployment knowledge of each node. Du *et al.*[10] described a model, in which the sensor nodes are deployed in groups, so in each group the nodes have high probability to be near to each other. So the basic idea is to let the nodes deployed near to each other select keys from sub-key pools that share more keys. In the scheme, because each node carries fewer keys, the memory efficiency and resilience are both improved.

3.2 Polynomial-based key pre-distribution schemes

Blundo *et al.*[11] proposed a polynomial-based key pre-distribution protocol, which is the basis of pairwise keys pre-distribution schemes.

To pre-distribute pairwise keys, one offline key set-up sever randomly generates a bivariate t-degree polynomial $f(x,y) = \sum_{i,j=0}^{t} a_{ij}x^iy^i$ over a finite field F_q. where q is a prime number that is large enough to accommodate a cryptographic key, and has the property of $f(x,y) = f(y,x)$. For each sensor i with a unique ID, the set-up server computes a polynomial share of $f(x,y)$, that is, $f(i,y)$. For any two sensor nodes i and j, node i can compute the common key $f(i,j)$ by evaluating $f(i,y)$ at point j, and node j can compute the common key with i by evaluating $f(j,y)$ at i. So to establish a pairwise key both nodes need to evaluate the polynomial with the ID of the other node. The scheme is proved secure and t-collusion resistant.

Liu and Ning[12] proposed a special scheme for sensor networks based on [11]. The main difference of this scheme with those in Section 3.1 is that it changes the global key pool to global polynomial pool. A pool of randomly generated bivariate polynomials is used to establish pairwise keys between sensors. So the nodes select different polynomials from the polynomial pool, in which each polynomial with different ID. In the direct key establishment phase, sensor nodes exchange the ID of polynomials to find shared polynomials, and so establish the pairwise key by computation as discussed in [11]. Compared with previous methods, this scheme is more secure. More important improvement is that the scalability is excellent, that is, sensors can be added dynamically without having to contact the previously deployed sensors.

A grid-based scheme is also proposed in [12], where the polynomials are arranged in a grid. The set-up server assigns each sensor in the network to a unique intersection in the grid. This grid-based method is described as low communication overhead, and is more intrusion tolerant than previous schemes.

The location information can be used to improve the polynomial-based key pre-distribution schemes, as proposed in [13], called the closest polynomial scheme. This scheme combines the expected locations of sensor nodes with the random subset assignment scheme in [12], and allows tradeoff between the security against node captures and the probability of establishing direct keys with a given memory constraint.

In all the polynomial-based key pre-distribution schemes, the essential computation in sensor nodes lies in the evaluation of a t-degree polynomial.

3.3 Blom′s matrix-based key pre-distribution schemes

The original matrix-based key pre-distribution scheme is proposed by Blom[14]. In this scheme, a symmetric matrix $K_{n\times n}$ stores all pairwise keys of a group of n nodes, where each element k_{ij} is the key between node i and node j. $K = (DG)^{\mathrm{T}}G$, where $D_{(\lambda+1)\times(\lambda+1)}$ is symmetric and $D_{(\lambda+1)\times n}$ is called public matrix, and $(DG)^{\mathrm{T}}$ is called secret matrix. Each node i stores the ith row of secret matrix and the ith column of public matrix G. After deployment, each pair of nodes i and j can individually compute a pairwise key $k_{ij} = k_{ji}$ by only exchanging their columns in plain text because the key is dot product of their own row and the column of other′s. Blom′s scheme has the λ-security. That is given one row compromised, no other is revealed. Only when more than λ rows are compromised, the entire secret matrix can be derived or broken by adversaries.

Yu and Guan[15] presented a group-based key pre-distribution scheme using sensor deployment knowledge based on [14]. This scheme distributes secret information instead of secret keys in sensor nodes to generate pairwise keys for nodes. Because most neighbors of a node are from its own group and neighboring groups, this scheme assigns each group a distinct secret matrix and makes neighboring groups share some other secret matrices, so that pairwise keys can be efficiently generated for neighboring nodes.

To use the location information, sensor field is divided into hexagonal grids. Accordingly, sensor nodes are divided into groups each of which is deployed into a grid. By using location knowledge, the resulting scheme has a high degree of connectivity and low memory requirement. At the same time it shows a good resilience against node capture.

By relaxing the requirement of Blom′s method[14] from a complete node graph to connected graph, another improved scheme was proposed by Du *et al.*[16]. The nodes that do not share a common key may still connect to each other by setting up the path key. In this way, the keys need to be stored become less, so the memory efficiency and resilience to sensor node capture are improved.

For the assumption of random capture is thought as too weak, a grid-group scheme is proposed to improve the security against the selective capture[17]. This scheme uniformly deploys sensors in a large area and systematically distributes secret keys to each sensor from a structured key pool. By using deployment knowledge, this scheme shows a good quality of resistant to selective node capture, and its memory usage is efficient.

3.4 Deterministic key pre-distribution schemes

Above key pre-distribution schemes are all based on the probabilistic approaches. Recently Lee and Stinson[18] have proposed the deterministic schemes to improve the resilience against node capture. This approach can support large size of sensor network.

In the deterministic scheme, the sensor network is modeled as a complete bipartite graph rather than a random graph. Each sensor node is assigned a unique ID. The basic idea of the deterministic scheme is that the edges of graph G are decomposed into star-like sub-graphs in which each vertex is a centre of one star and a leaf of $r/2$ distinct stars. For a sensor node u, it will receive two secret keys: one is K_u, which is gotten from the key pool $\mathcal{K}$, another is a "hashed" key $h(K_v||ID(u))$, if it is contained in a star-like sub-graph centered at v. Here h is a public one-way function. Since a node v can compute $h(Kv||ID(u))$ by evaluating function h at the concatenation of its unique key K_v and public ID of u, $ID(u)$, both u and v can establish their secret key $h(Kv||ID(u))$.

The scheme is efficient in memory usage since each node u only contains $r/2+1$ keys (one secret key K_u and $r/2$ hashed keys). At the same time, the scheme can achieve the "perfect resiliency" since when one node u is captured by adversary, only K_u and $r/2$ hashed keys $h(Kvi||ID(u))$ for adjacent nodes v_i can be gotten. Based on the one-way hash function h, it is infeasible to know the K_{vi}. So the links between any two non-captured nodes are not compromised.

To meet the requirement of large size sensor network, a multiple ID-based one-way function scheme is proposed based on the basic ID-based one-way function scheme. Though there is no more perfect resiliency, the multiple ID-based one-way function scheme provides a trade-off between network size and resiliency against adversary attack.

By modifying Blom′s scheme[14] on complete bipartite graphs, a deterministic multiple space scheme[18] was also described by Lee and Stinson[18]. The deterministic key pre-distributed scheme shows stronger resiliency compared to some probabilistic key pre-distribution schemes[12].

4 Additional requirements and further research directions

Based on the investigation and discussion of current schemes proposed on the key management issues in wireless sensor networks, we may consider some possible improvement areas.

One area is more intensive research on path-key establishment methods. One of the main phases of key pre-distribution schemes is establishing the path between the two nodes that do not share common keys directly. Some special protocols combined with routing information may be considered to achieve the secure and efficient path-key establishment. Furthermore, based on the current research on the coverage and connectivity in the sensor networks, some random distribution model[19] should also be considered when modeling a secure communication model in wireless sensor networks.

Another area is how to modify the public key cryptography and apply it to the key management issues. Recent studies show that it is still possible to apply public key to sensor networks by selecting right algorithm and associated parameters[20]. With the advancements of hardware and software, public key infrastructure in WSN is not only possible but also necessary[21].

Besides, on some special condition where an always trusted entity (*e.g.*, the gateway[22] or command node[23]) exits in the sensor network, the arbitrated keying protocols are still be implemented.

The Shamir′s secret sharing theory[24] may be used to build a secret key sharing scheme to tolerate the capture of some sensor nodes.

Most of the current proposed key management schemes are based on the assumption that all the nodes in the sensor networks are homogeneous and with similar capabilities, such as memory and radio range. Some research has found that by applying heterogeneous sensor nodes in a sensor network, the small percentage of more capable sensor nodes can provide an equal level of security meanwhile improve the resilience of node compromise. The unbalanced scheme proposed in [25] not only reduces the number of transmissions necessary to establish session-keys but also reduces the effects of both single and multiple node captures.

5 Conclusion

Key management is a fundamental security issue in sensor networks. It is the basis to establish the secure communication using cryptographic technologies between sensor nodes in a sensed area. However, due to the current resource constraints on sensors, it is infeasible to use traditional key management techniques such as public key cryptography or key distribution center based protocols. So the key pre-distribution schemes are paid most attention in the key management area.

Current key pre-distribution schemes can be classified into four classes: pure probabilistic key pre-distribution schemes, polynomial-based key pre-distribution schemes, Blom′s matrix-based key pre-distribution schemes and deterministic key pre-distribution schemes. Each kind of schemes has its advantages and application environment.

An obvious rule can be drawn from these proposed schemes is that the location knowledge can be used to improve the performance of the key management schemes, such as the connectivity, resilience against nodes capture and memory efficiency.

From the discussion, we can also see that most of the key management solutions for wireless sensor networks are trying to find the better tradeoffs between system security (*e.g.*, resilience to node capture) and network connectivity. All of them have weak and strong points. The diverse usages of wireless sensor networks make it unreasonable to try to find the single perfect scheme suitable for all situations.

References

1 Akyildiz I F, Su W L, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. *IEEE Communications Magazine*, 2002, **40**(8): 102∼114

2 Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks, *Communications of the ACM, Special Issue on Wireless Sensor Networks*, 2004, **47**(6): 53∼57

3 Law Y W, Etalle S, Hartel P H. Key management with group-wise pre-deployed keying and secret sharing pre-deployed keying. Technical report (TR-CTIT-02-25), The Netherlands: Centre for Telematics and Information Technology, University of Twente, 2002

4 Carman D W, Kruus P S, Matt B J. Constraints and approaches for distributed sensor network security. Technical report, NAI Labs, 2000

5 Traynor P, Cao G, Porta T F. The effects of probabilistic key management on secure routing in sensor networks. Networking and Security Center Technical Report NAS-TR-0003-2005, Penn State: Department of Computer Science and Engineering, Penn State University, 2005

6 Eschenauer L, Gligor B D. A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM Conference on Computer and Communication Security. Washington, DC, USA: 2002. 41∼47

7 Spencer J. The Strange Logic of Random Graphs, Algorithms and Combinatorics. Number 22, Springer-Verlag, 2000

8 Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proceedings of IEEE Symposium on Security and Privacy, Berkeley, California: IEEE Press, 2003. 197∼213

9 Huang C, Du D. New constructions on broadcast encryption and key pre-distribution schemes. In: Proceedings of IEEE INFOCOM′05. Miami: IEEE Press, 2005. 515∼523

10 Du W, Deng J, Han Y S, Chen S, Varshney P K. A key management scheme for wireless sensor networks using deployment knowledge. In: Proceedings of IEEE INFOCOM′04. Hong Kong: IEEE Press, 2004. 586∼597

11 Blundo C, Santix A D, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-secure key distribution for dynamic conferences. In: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, Berlin: Spring-Verlag, 1992. 471∼486

12 Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In: Proceedings of 10th ACM Conference on Computer and Communications Security (CCS′03). Washington DC: ACM Press, 2003. 41∼47

13 Liu D, Ning P. Improving key pre-distribution with deployment knowledge in static sensor netowrks. ACM Transactions on Sensor Networks, 2005, **1**(2): 204∼239

14 Blom R. An optimal class of symmetric key generation systems. In: Proceedings of the Eurocrypt 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques. Springer Verlag, 1985. 335∼338

15 Yu Z, Guan Y. A robust group-based key management scheme for wireless sensor networks. In: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC 2005). New Orleans, LA USA: IEEE Press, 2005. 13∼17

16 Du W, Deng J, Han Y S, Varshney P, Katz J, Khalili A. A pairwise key pre-distribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 2005, **8**(2): 228∼258

17 Huang D, Mehta M, Medhi D, Harn L. Location-aware key management scheme for wireless sensor networks. In: Proceedings of ACM Workshop on Security of *Ad Hoc* and Sensor Networks (SASN′04). Washington DC, USA: ACM Press, 2004. 29∼42

18 Lee J, Stinson D R. Deterministic key predistribution schemes for distributed sensor networks. In: Proceedings of ACM Symposium on Applied Computing 2004, Lecture Notes in Computer Science 3357 (2005), Waterloo, Canada: Springer, 2004. 294∼307

19 Bettstetter C. On the minimum node degree and connectivity of a wireless multihop network. In: Proceedings of the 3rd ACM International Symposium on Mobile *Ad hoc* Networking & Computing′02, EPF Lausanne, Switzerland: ACM Press, 2002. 80∼91

20 Gaubatz G, Kaps J, Sunar B. Public key cryptography in sensor networks - revised. In: Proceedings of 1st European Workshop on Security in *Ad-hoc* and Sensor Networks (ESAS 2004). Heidelberg, Germany: Springer, 2004. 2∼18

21 Arazi B, Elhanany I, Arazi O, Qi H. Revisiting public-key cryptography for wireless sensor networks. *Computer*, 2005, **38**(11): 103∼105

22 Jolly G, Kusçu M, Kokate P, Younis M. A low-energy key management protocol for wireless sensor networks. In: Proceedings of 8th IEEE International Symposium on Computers and Communications. Washington DC, USA: IEEE Computer Society, 2003. 335

23 Eltoweissy M, Younis M, Ghumman K. Lightweight key management for secure wireless sensor networks. In: Proceedings of IEEE Workshop on Multi-hop Wireless Networks, Phoenix, Arizona: IEEE Press, 2004. 813∼818

24 Shamir A. How to share a secret. *Communications of the ACM*, 1979, **22**(1): 612∼613

25 Traynor P, Choi H, Cao G, Zhu S, La Porta T F. Establishing pair-wise keys in heterogeneous sensor networks. Networking and Security Center Technical Report NAS-TR-0001-2004. Penn State: The Department of Computer Science and Engineering, Penn State University, 2004

SUN Dong-Mei Received her master degree in control engineering from Beijing University of Technology in 1995 and Ph. D. degree in signal & information processing from Northern Jiaotong University in 2003. Currently she is an associate professor at the Institute of Information Science, Beijing (original Northern) Jiaotong University. Her research interests include information security, biometrics recognition, pattern recognition, and image processing.

HE Bing Received his bachelor degree in communication engineering and master degree in signal & information processing from Northern Jiaotong University of China in 2000 and 2003, respectively. He joined Honeywell Technology Solutions Lab, China in 2003. Currently, he is a Ph. D. candidate in Electrical & Computer Engineering and Computer Science Department at University of Cincinnati. His research interests include wireless mesh networks, 802.16 protocol and wireless network security.