무선 센서 네트워크에서 분산 클러스터링을 이용한 안전한 에너지 효율적인 라우팅 기술★

천은홍* · 이연식**

요 약

무선 센서 네트워크은 폭넓은 다양한 응용에서 경제적으로 성공할 수 있는 모니터링 솔루션이다. 그러나 악의적이거나 감시하는 사람이 없는 환경에서 침입을 인식하고 방지하며 안전하고 에너지 효율적인 것을 보장하는 네트워크를 통한 정보의 안전한 전송은 주된 도전이다. 이에 따라, 이 논문은 집적된 데이터의 무결성, 인증성과 비밀성을 보장하기 위하여 안전한 무선 센서 네트워크에 필수적인 보호를 포함하는 분산 클러스터링 프로세스를 제안한다. 안전한 키 관리 스킴을 위하여 대칭형과 비대칭형 키의 전단계 분산의 개념을 사용하고, 클러스터 내에 있는 각 센서 노드가 배치되기 전에 암호화를 위한 전단계 분산 매개변수를 사용하는 센서 네트워크 토폴로지에 기초한 계층적 클러스터에 대한 상세한 스킴에 대하여 기술한다. 마지막으로 무선 센서 네트워크에서 제안된 스킴의 성능 시험 결과를 보인다.

A Secure Energy-Efficient Routing Scheme Using Distributed Clustering in Wireless Sensor Networks

EunHong Cheon* · YonSik Lee**

ABSTRACT

The wireless sensor networks have become an economically viable monitoring solution for a wide variety of civilian and military applications. The main challenge in wireless sensor networks is the secure transmission of information through the network, which ensures that the network is secure, energy-efficient and able to identify and prevent intrusions in a hostile or unattended environment. In that correspondence, this paper proposes a distributed clustering process that integrates the necessary measures for secure wireless sensors to ensure integrity, authenticity and confidentiality of the aggregated data. We use the notion of pre-distribution of symmetric and asymmetric keys for a secured key management scheme, and then describe the detailed scheme which each sensor node within its cluster makes use of the pre-distribution of cryptographic parameters before deployment. Finally, we present simulation results for the proposed scheme in wireless sensor network.

Key words : wireless sensor network, key management, distributed clustering, authenticity, energy efficient routing

접수일(2016년 08월 25일), 게재확정일(2016년 09월 20일)

★ 본 논문은 2016년도 우석대학교 교내학술연구조성비 지원에 의하여 연구되었음.

* 우석대학교/컴퓨터공학과
** 군산대학교/컴퓨터정보공학과

1. Introduction

Wireless sensor networks(WSN) are some of the fastest growing technologies. They consist of spatially distributed autonomous sensors wirelessly connected in order to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to jointly pass their data through the network to a main location. Military and commercial applications such as traffic monitoring, environmental measurements and patient health monitoring can be easily implemented using wireless sensor networks. However as the application becomes distinct, architectures and requirements may become more complex. WSNs in general and in nature are unattended and physically accessible, therefore, sensors which are battery powered may die and the network will be stopped from performing its task; hence the need of a network that can last as long as possible. They could be vulnerable to traffic analysis attacks which can lead to the disclosure of the information sensed and relayed. It is necessary for WSNs to have an energy efficient protocol and security measures in place to prevent an intruder from analyzing the traffic and introducing compromised nodes in order to decimate or disturb the network performance and lifetime. Classic prevention measures, such as encryption and authentication, can be used in wireless sensor networks. However, they cannot eliminate every threat. We propose in this thesis a distributive clustering method for an energy efficient routing protocol in hierarchical cluster-based WSNs for the secure flowing of the sensor readings, until the destination is reached.

In this paper, by adopting the characteristics of Heed protocol, we present a secure distributed energy-efficient architecture for wireless sensor networks. We give a detailed description of our method by using both symmetric and public cryptography. The rest of the paper is organized as follows. In section 2, we introduce related solutions of hierarchical clustering problem. Section 3 presents our proposal to the distributed clustering for energy efficient routing. In section 4, we present simulation results. Finally, conclusions and directions for future research are identified in section 5.

2. Related Works

The clustering in wireless sensor network is one of the solutions to achieve better scalability, energy efficiency, channel access, routing, data aggregation and many others.

In previous years, many Leader-First cluster formation protocols have been proposed by selecting the cluster heads based on one or multiple metrics, such as node connectivity, node mobility and residual energy[1][2]. Several cluster formation protocols have been proposed by considering the cluster heads selection problem as a special case of finding the minimum dominating set problem[3][4][5]. Two secure clustering formation algorithms are proposed for wireless ad hoc networks[6][7].

Another interesting research area is key management in WSN where one of the classification criterions includes pre-distribution[4], or post distribution of secret keys. Recent research suggests that symmetric secret key pre-distribution is possibly the only practical approach for establishing secure channels among sensor nodes[8]. To bootstrap security using Eschenauer and Gligor's original scheme, a network goes through three phases. In the key pre-distribution phase, which takes place prior to network deployment, a large pool of keys and their IDs are generated[9]. Each node is then assigned a ring of keys, drawn from the pool at random, without replacement. In the shared-key discovery phase, which takes place during network setup, all nodes broadcast the IDs of the keys on their key rings. Through these broadcasts, a node finds out with which of their neighbors they share a key. These keys can then be used for establishing secure links between the two neighbors[10]. Finally, during the path-key establishment phase, pairs of neighboring nodes that do not share a key can set up their own keys, as long as they are connected by two or more secure links at the end of shared key discovery. Because of the way keys are assigned, a key can be found in more than two nodes, and used in multiple communication links. When a node is compromised, all its keys, and all the links secured by these keys are also compromised. The Hybrid energy-efficient distributed(Heed) clustering is a novel approach for cluster based energy-efficient WSN protocol that has the characteristic of prolonging the network lifetime by distributing energy consumption also producing well distributed cluster heads and compact cluster[2][6][11]. Heed protocol elects cluster heads that are rich in residual energy. This minimizes the energy consumption by avoiding all the nodes needing to send data to a distant base station. Heed is fast and has low overhead, provides other features, such as load balancing.

3. The Proposed Distributed Clustering

The proposed secure distributed clustering method presented in this paper is based on the following criteria: key pre-distribution, intra-cluster key establishment using symmetric cryptography, inter-cluster key establishment using asymmetric cryptography, and finally cluster head clique formation for misbehavior detection. We use both key pre- distribution and symmetric cryptography, because of the resource constraints that characterize WSN. We also make use of asymmetric cryptography for communication between the base station(BS) and cluster heads(CH). Public and symmetric key infrastructures are considered for encryption and decryption; message authentication code(MAC) is also used for integrity purposes.

3.1 Key pre-distribution

Before deployment for secure clustering, each sensor is loaded with the following parameters.

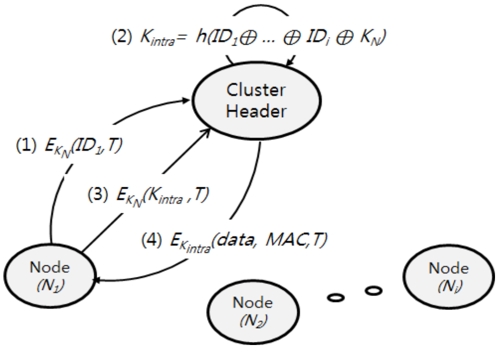
- The BS public key($K_{PU_{BS}}$) is loaded into the sensor as the corresponding private key is held at the BS, which will be used to establish a secure communication with the BS and provide BS authentication.
- A unique identifier for the node ID_i
- The network system manger will also generate another couple of public and private keys (K_{PRi}, K_{PUi}) for each sensor, which will be used against cluster head repudiation when transmitting the cluster head clique to the BS. Only the private key is loaded into the sensor.
- A symmetric network key(K_N) serves as the initial trust for the joining of the clusters in the network and later used to compute the intra-cluster key, inter-cluster key and finally in distance mapping, which will be applied to generate the rotating network key.

A symmetric key cryptography method such as message authentication code(MAC) is used between nodes for message integrity to fulfill the lower power demand. Messages are encrypted when joining the cluster head with the network key initially generated by the network manager, the computed inter-cluster key, and the computed intra-cluster key and finally a MAC is generated for the integrity of data between nodes, and between cluster head and BS.

3.2 Cluster Formation and Intra Cluster Communication

We first use the hybrid process to select cluster-heads according to Heed protocol. Once the cluster heads have been selected, nodes join the cluster formation process by encrypting hello messages with the network key after cluster head broadcast. After that the newly selected cluster head starts a process to compute the intra cluster communication key based on node's ID for the session that will serve for communication within the cluster as described below: $K_{intra}= h(ID_i \oplus \cdots \oplus ID_{i+n-1} \oplus K_N)$ represents nodes within the cluster range. The resulting key is the intra cluster key.

Figure 1 shows the intra-cluster communication, and Figure 2 describes the processes of cluster formation and intra cluster communication, respectively.


(2) $K_{intra}= h(ID_1 \oplus \ldots \oplus ID_i \oplus K_N)$
Cluster Header
(1) $E_{K_N}(ID_1, T)$
(3) $E_{K_N}(K_{intra}, T)$
(4) $E_{K_{intra}}(data, MAC,T)$
Node (N_1)
Node (N_2)
Node (N_i)

(Figure 1) Intra cluster communication

```
Elect Cluster_Heads()
For (i=1, n)
    Send $E_{K_N}$ ($ID_i$, T) from $N_i$ to CH
CH generates member_node_list();
CH computes $K_{intra}=h(ID_i \oplus \cdots \oplus ID_{i+n-1} \oplus K_N)$
For (i=1, n)
    send $E_{K_N}(K_{intra}, T)$ from CH to $N_i$.
    Ni reads (data) and  generates (MAC)
    Send $E_{K_{intra}}$(data, T, MAC) from Ni to CH
CH checks (T) and verifies (MAC);
CH performs Data_aggregation();
```

(Figure 2) Processes of cluster formation and intra cluster communication

3.3 Inter Cluster Communication

Just like the intra cluster key computation, the inter cluster communication key is also generated by the following process when the cluster head clique is formed. $K_{inter}= h(ID_{CH1} \oplus \cdots \oplus ID_{CHn} \oplus K_N)$ represents the set of all the alive CH forming the network. The resulting key is used for communication between clusters after the cluster formation and clique verification process.

After the clustering

Once CH has selected the information to forward, it finds the destination first.

a) Case base station: at this stage we consider that all keys are generated yet, CH encrypt the packet with $K_{PU_{BS}}$, then sign the message and add a timestamp along with a MAC according to the set of predefined rules.

b) Case cluster head: it encrypts the message with the inter cluster key and adds a time stamp and a MAC. The receiving CH will be able to check the integrity of the corresponding readings before forwarding it to the BS according to the protocol rules.

3.4 Cluster Head Clique Formation

The clique formation process is initiated to make sure that the newly elected CH is authorized member of the network and that there are no intruders among them. In our protocol, cluster heads carry the entire list of their members along with their IDs. At the end of the cluster head clique formation, the cluster with the most energy is elected to connect with the BS. The BS will verify all node identities and thus provide resilience against node replication.

In order for this to occur, CH determine among themselves the CH with most residual energy and connectivity degree by simple message exchange, to initiate the clique formation process, which is achieved in 4 rounds:

a) Every CH has a routing table that stores prior knowledge of its neighbor CH, which is used to connect within a single hop with a minimal energy level. Each CH exchanges its neighbor CH list with its neighbor CHs and computes the local maximum clique.

b) CHs exchange their local clique and adjust the maximum clique accord-ing to the received local maximum clique.

c) CHs exchange their updated clique between neighbor CHs and derive their final clique.

d) CHs exchange their final clique for comparison to check for inconsistencies. The one with the most residual energy will then forward the clique to the BS for cluster head clique identification.

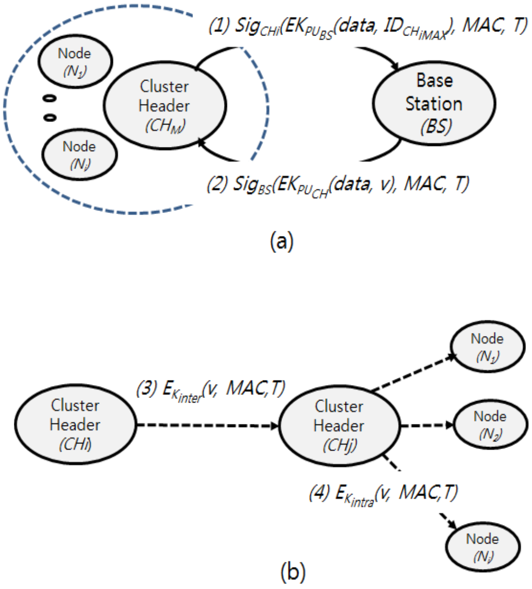
If nothing is detected and the BS response is received according to the predefined set of rules the process successfully terminates with a clique agreement.

```
Form Cluster-Head Network()
$CH_M$ generates cluster_head_list()
$CH_M$ computes $K_{intra}=h(ID_i \oplus \cdots \oplus ID_{i+n-1} \oplus K_N)$
Send [$Sig_{CHi}(EK_{PU_{BS}}(CH_{list}, MAC, T))$] from $CH_M$ to BS
If (success),
    send [$Sig_{BS}(EK_{PU_{CH_M}}(v, MAC, T))$] from BS to $CH_M$
Begin data_transmission()
```

(Figure 3) Process of cluster head clique

After the clique formation, the CH with the most connectivity and the required minimum energy will forward the clique list to the BS by a message containing its ID, all signed with the CH private key and then the network symmetric key. The BS after authenticating and approving the received list will send the response encrypted with the sender CH public key all again encrypted with the BS private key. This is followed by a broadcast of the response to the CH, which in turn broadcasts the response parameters to their respective cluster. After that, data transfer can start from SN to CH. CH will communicate by encrypting and sending data with the inter cluster key.

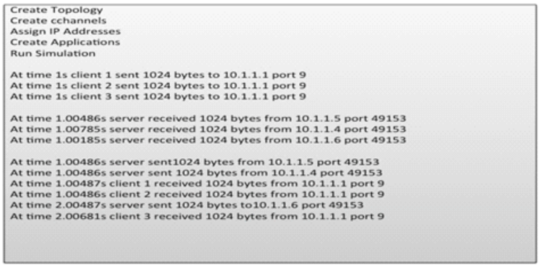
The approval response from the BS will contain another parameter 'v' that will serve as an initial vector for the Distance Mapping function DM when rotating the network key, as illustrated in Figure 4. $K_N=DM(K_N, v)$ become the new key at the next clustering process.


(1) $Sig_{CHi}(EK_{PU_{BS}}(data, ID_{CH_{iMAX}}), MAC, T)$
Node (N_1)
Cluster Header (CH_M)
Node (N_i)
Base Station (BS)
(2) $Sig_{BS}(EK_{PU_{CH}}(data, v), MAC, T)$
(a)
Cluster Header (CHi)
(3) $E_{K_{inter}}(v, MAC,T)$
Cluster Header (CHj)
Node (N_1)
Node (N_2)
(4) $E_{K_{intra}}(v, MAC,T)$
Node (N_i)
(b)

(Figure 4) Communication between base station and cluster head

4. Evaluations

At the base of the NS3 network simulator, a applications have been implemented. A socket application agent is executed by an ad-hoc network where nodes are wirelessly connected by the 802.11 norms and organize themselves into three clusters with three cluster heads. This illustrates the communication scheme used in Intra-cluster communication where Hello messages are sent and as the result, the intra-cluster key is generated. We present that message exchange session to show how packets are sent and received by a node and its cluster head. We consider an ad hoc network where three stations act as cluster heads and the other nodes organize themselves to communicate with one of the cluster heads. The 3 cluster heads receive packets (Hello messages) from all member nodes and acknowledge with another packet representing the intra-cluster session key. The simulation result with NS3 is shown in Figure 5, and a view of the PCAP files of one Cluster-head is Figure 6.



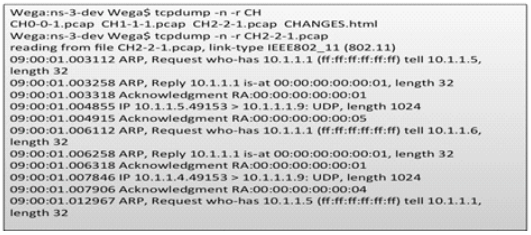
```
Create Topology
Create cchannels
Assign IP Addresses
Create Applications
Run Simulation

At time 1s client 1 sent 1024 bytes to 10.1.1.1 port 9
At time 1s client 2 sent 1024 bytes to 10.1.1.1 port 9
At time 1s client 3 sent 1024 bytes to 10.1.1.1 port 9

At time 1.00486s server received 1024 bytes from 10.1.1.5 port 49153
At time 1.00785s server received 1024 bytes from 10.1.1.4 port 49153
At time 1.00185s server received 1024 bytes from 10.1.1.6 port 49153

At time 1.00486s server sent1024 bytes from 10.1.1.5 port 49153
At time 1.00486s server sent 1024 bytes from 10.1.1.4 port 49153
At time 1.00487s client 1 received 1024 bytes from 10.1.1.1 port 9
At time 1.00486s client 2 received 1024 bytes from 10.1.1.1 port 9
At time 2.00487s server sent 1024 bytes to10.1.1.6 port 49153
At time 2.00681s client 3 received 1024 bytes from 10.1.1.1 port 9
```

(Figure 5) Simulation for inter-cluster message exchange



```
Wega:ns-3-dev Wega$ tcpdump -n -r CH
CH0-0-1.pcap  CH1-1-1.pcap  CH2-2-1.pcap  CHANGES.html
Wega:ns-3-dev Wega$ tcpdump -n -r CH2-2-1.pcap
reading from file CH2-2-1.pcap, link-type IEEE802_11 (802.11)
09:00:01.003112 ARP, Request who-has 10.1.1.1 (ff:ff:ff:ff:ff:ff) tell 10.1.1.5,
length 32
09:00:01.003258 ARP, Reply 10.1.1.1 is-at 00:00:00:00:00:01, length 32
09:00:01.003318 Acknowledgment RA:00:00:00:00:00:01
09:00:01.004855 IP 10.1.1.5.49153 > 10.1.1.1.9: UDP, length 1024
09:00:01.004915 Acknowledgment RA:00:00:00:00:00:05
09:00:01.006112 ARP, Request who-has 10.1.1.1 (ff:ff:ff:ff:ff:ff) tell 10.1.1.6,
length 32
09:00:01.006258 ARP, Reply 10.1.1.1 is-at 00:00:00:00:00:01, length 32
09:00:01.006318 Acknowledgment RA:00:00:00:00:00:01
09:00:01.007846 IP 10.1.1.4.49153 > 10.1.1.1.9: UDP, length 1024
09:00:01.007906 Acknowledgment RA:00:00:00:00:00:04
09:00:01.012967 ARP, Request who-has 10.1.1.5 (ff:ff:ff:ff:ff:ff) tell 10.1.1.1,
length 32
```

(Figure 6) PCAP file of participating node.

5. Conclusions

In this paper, we described a secure distributed clustering process based on Heed protocol using the notion of pre-distribution cryptographic keys for secured key management as it is the first breach an attacker can cross. We then proposed the detailed scheme to be deployed on a cluster based WSN topology. Sensors are loaded with initial trust value, which a set of parameters loaded before deployment and after the first clustering operation, the sensors apply a distance mapping function to compute the new symmetric network key for cluster formation at the beginning of each round. The proposed secure distributed cluster process dynamically generates inter and intra cluster path symmetric link keys in combination with the cluster head clique, that is, a list of cluster heads for each round authenticated by the base station. Our key management scheme performs other random key pre-distribution protocols in that less space is required. This is due to the reduced number of keys instead of a big pool of full keys stored in each sensor producing lower communication overhead, as the path-key establishment phase does not require a lot of computation. Our scheme also offers very high resilience against node capture and node replication. In brief, the proposed method adapts to the constraints of WSN, while maintaining a different level of security at every stage. Our future work will focus on reducing the communication overhead between cluster heads and the base station and also more rapid regeneration of keys in order to strengthen the resilience against node capture.

References

[1] B. Parno, A. Perrig, and V. Gligor. "Distributed detection of node replication attacks in sensor

networks," IEEE Symposium on Security and Privacy, pp. 1-5, 2009.

[2] Younis, O. and Fahmi, S. "Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Transactions on Mobile Computing, Vol. 3, No. 4 pp. 366-379, 2004.

[3] Lalita Yadav et al, "Low Energy Adaptive Clustering with Deterministic Cluster Head Selection," International Journal of Computer Science and Information Technologies, Vol. 5, No. 3, pp. 4661-4664, 2014.

[4] Aslam, M. Javaid, N. Rahim, A. Nazir, "Survey of Extended LEACH-Based Clustering Routing Protocols for Wireless Sensor Networks," IEEE Conference on Embedded Software and Systems, pp. 1232-1238, 2012.

[5] S. P. Barfunga, P. Rai, and H. K. Sarma, "Energy efficient cluster based routing protocol for wireless sensor network," IEEE Conferences on Computer and Communication Engineering, pp. 603-607, July. 2012.

[6] W. Gu, S. Chellappan, X. Bai, and H. Wang, "Scaling laws of key pre-distribution protocols in wireless sensor networks," Information Forensics and Security, IEEE Transactions on, Vol. 6, No. 4, pp. 1370-1381, 2011.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," Proceedings of the 9th ACM conference on Computer and Communications Security, pp. 41 - 47, 2002.

[8] H. M. Sun, M. E. Wu, M Jason Hinek, C. T. Yang and V. S. Tseng, "A pairwise key establishment for wireless sensor networks," Journal of Systems and Software, Vol. 82, No. 9, pp. 1503-1512, 2009.

[9] C. Dhivya Devi et al. "study on security protocol in wireless sensor networks," International Journal of Engineering and Technology, Vol. 5, No. 1, 2013.

[10] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," IEEE International Workshop on Sensor Network Protocols and Applications, pp.293-315, 2003.

[11] Raed M. Bani Hani and Abdalraheem A. Ijjeh, "A Survey on LEACH-Based Energy Aware Protocols for Wireless Sensor Networks," Journal of Communications, Vol 8, No 3, pp. 192-206, 2013.

[저자소개]

천 은 홍 (Eun-hong Cheon)

1981년 2월 광운대학교
응용전자공학과 학사
1985년 2월 아주대학교
전자공학과 석사
1998년 8월 아주대학교
컴퓨터공학과 박사
1988년 9월~현재: 우석대학교
컴퓨터공학과 교수

email : ehcheon@woosuk.ac.kr

이 연 식 (Yon-sik Lee)

1982년 2월 전남대학교
전자계산학과 학사
1984년 2월 전남대학교
전자계산학과 석사
1994년 2월 전북대학교
전산응용공학 박사
1986년 3월~현재: 군산대학교
컴퓨터정보공학과 교수

email : yslee@kunsan.ac.kr