韓國컴퓨터情報學會 論文誌
第17卷 第2號, 2012. 2.

2012-17-2-3-5

A Sextant Cluster Based Monitoring on Secure Data Aggregation and Filtering False Data in Wireless Sensor Networks

Anuparp Boonsongsrikul *, Seung-Kyu Park *, Seung-Hun Shin **

무선센서 네트워크에서의 육분원 방식 모니터링 기반 안전한 데이터 병합 및 위조 데이터 필터링

Anuparp Boonsongsrikul *, 박 승 규*, 신 승 훈**

Abstract

Local monitoring is an effective technique in securing data of wireless sensor networks. Existing solutions require high communication cost for detecting false data and this results in a network lifetime being shortened. This paper proposes novel techniques of monitoring based secure data aggregation and filtering false data in wireless sensor networks. The aim is to reduce energy consumption in securing data aggregation. An aggregator and its monitoring node perform data aggregation in a 60^{o} sextant cluster. By checking Message Authentication Codes (MAC), aggregation data will be dropped by a forward aggregator if data aggregated by the aggregator and data monitored by the monitoring node are inconsistent. The simulation shows that the proposed protocol can reduce the amount of average energy consumption about 64% when comparing with the Data Aggregation and Authentication protocol (DAA)[1]. Additionally, the network lifetime of the proposed protocol is 283% longer than that of DAA without any decline in data integrity.

▸ Keyword : Sensor Networks, Data Aggregation, Energy Consumption, Data integrity, Monitoring

요 약

무선 센서 네트워크에서 지역 감시는 데이터를 보호하는 효과적인 방법이지만 기존의 방법은 위조 데이터를 탐지하는데 많은 통신 부하를 요구하며, 이는 네트워크 수명을 단축시키는 결과를 야기한다. 따라서 본 논문에서는 시

• 제1저자 : Anuparp Boonsongsrikul • 교신저자 : 박승규
• 투고일 : 2011. 09. 14, 심사일 : 2011. 09. 19, 게재확정일 : 2011. 10. 11
* 아주대학교 정보통신공학과(Dept. of Information and Communication, Ajou University)
** 아주대학교 정보컴퓨터공학부(Div. of Information and Computer, Ajou University)

큐어 데이터 병합에 소요되는 에너지 소모 저감을 목적으로 하는 새로운 감시 기반 시큐어 데이터 병합 및 허위 데이터 필터링 방법을 제안한다. 제안된 방법에서 애그리게이터와 이의 감시 노드는 60°의 내각을 갖도록 분할된 육분원형 클러스터를 기반으로 데이터 병합을 수행한다. 그리고 데이터 병합 과정에서 메시지 인증 코드(MAC)의 비교를 통해 애그리게이터에 의해 병합된 데이터와 감시 노드에 의해 감지된 데이터가 불일치하는 것으로 판단되면 병합 데이터는 전달 애그리게이터에 의해 소거된다. 시뮬레이션에 의하면 제안된 방법은 평균 소모 에너지 측면에서 DAA 프로토콜에 비해 에너지 소모가 64% 감소되었음을 확인하였다. 또한 이를 통해 제안된 프로토콜은 DAA 프로토콜에 비해 네트워크 수명을 283% 연장 가능하며, 이 때 데이터 정확도 측면에서의 성능 저하는 없었다.

▸ Keyword : 센서 네트워크, 데이터 병합, 에너지 소모, 데이터 무결성, 감시

I. Introduction

Wireless sensor networks are applied in a wide range of applications to monitor, gather and analyze environments such as military surveillance, emergency response, forest fire monitoring, etc. However, energy is an extremely critical resource for battery-powered wireless sensor networks and security also becomes important when sensor nodes are deployed in a hostile environment. It is challenging to provide effective energy and security mechanisms against compromised nodes in wireless sensor networks.

Local monitoring is a promising mechanism in which many researchers[1-4] proposed an effective solution for securing wireless sensor networks. Among those of [1-4], the Data Aggregation and Authentication protocol (DAA)[1] can support data confidentiality, data aggregation and false data detection while work[2-3] reveal aggregation data. The work[4] does not support data aggregation. Therefore DAA is more effective than other works in terms of security and power consumption. The DAA provides data confidentiality that prevents against eavesdropping and data aggregation that reduces communication cost. However, it has a limitation where it requires a higher transmission range in detecting false data, which results in much consuming energy in sensor nodes.

This paper proposes a monitoring based secure data aggregation and filtering false data in wireless sensor networks. The objective of this paper is to minimize energy consumption in detecting false data. This approach adopts geographic routing protocols[5-6] to set up clusters where a cluster consists of an aggregator (cluster head) and at least T sensor nodes in a shade area as illustrated in Fig.1. The cluster is called "60° sextant cluster". Each aggregator and monitoring node performs aggregation data and Message Authentication Code (MAC). Aggregation data will be dropped by a forward aggregator, if the verification of MACs fails. The difference between DAA and our work is that monitoring node M in [1] should be able to overhear all neighboring nodes of aggregator Aj while monitoring node M in our work overhears all nodes in a 60° sextant cluster. Since the monitoring area of monitoring node M is more narrow than that of DAA, energy consumption of our proposed protocol is lower than that of DAA as indicated in the later sections.

The rest of this paper is organized as follows. Section II presents related work. Section III presents assumptions. Section IV presents a proposed scheme. Section V evaluates the effectiveness of our protocol and shows the simulation results. Section VI concludes the paper.

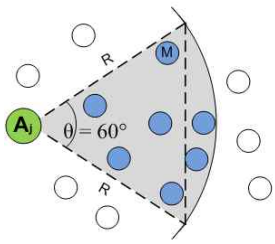

Fig. 1 A cluster model

II. Related work

Existing solutions based on monitoring[1-4] succeed in securing data but most of them require high communication cost. The following is a brief description of ideas and shortcomings for previous works.

De Silva proposed the Intrusion Detection System (IDS)[4]. When a monitoring node finds misbehavior of their neighboring nodes, it sends a reporting message to the base station. However this work requires high communication cost because it does not support data aggregation. Boonsongsrikul[2] proposed monitoring based secure data aggregation to defend against false data injection attacks. This work aims to identify the attacker. When a compromised node injects false data, many reporting messages of monitoring nodes are sent to the base station. Work[3] is proposed to reduce communication cost and energy consumption of work[2]. Instead of sending many reporting messages to the base station, reporting messages are summarized into a single report. The single report is then sent to the base station. The simulation shows that energy consumption of work[3] is 45% lower than that of work[2]. However, works [2], [3] and [11] have some limitations that they do not provide data confidentiality and dropping of false data. Therefore, aggregation data can be eavesdropped and sensor nodes waste their energy in sending false data.

Ozdemir and Cam [1] proposed a false data detection protocol that provides both data confidentiality and data aggregation. A monitoring node plays an important role to detect false data sent by an aggregator. A monitoring node can overhear all neighboring nodes of an aggregator. However, a monitoring node requires a higher transmission range in detecting false data and results in sensor nodes consuming much energy. As illustrated in Fig. 2, suppose DAA is designed that the transmission range of each node is 10 meters. To meet a requirement that monitoring node M can overhear all incoming data of aggregator A, monitoring node M and node C should have a sufficient transmission range. This means that the transmission range between monitoring node M and node C should be at least $10\sqrt{3}$ meters instead of 10 meters. This is more than 71% increase in a transmission range. Since the power consumption is proportional to the square of the transmission range, DAA increases in power requirements as shown in Section V.

III. Assumptions

1. Network model

A wireless sensor network is assumed as a large scale network with densely deployed sensor nodes. Some sensor nodes are dynamically selected as aggregators to aggregate data from their neighboring nodes. A sensor node is supposed to know its coordinate and neighboring nodes' coordinates (x,y). The geographic routing protocol[5-6] is adopted to establish a 60° sextant cluster consisting of an aggregator (cluster head) and at least T sensor nodes. The network topology consists of many clusters where two consecutive aggregators can communicate as illustrated in Fig. 3. An aggregator receives data sent by senor nodes in its cluster and performs data aggregation. The base station is the final destination for collecting aggregation data.

2. Pair-wise keys and group keys

Node i is assumed to share a pairwise key with node j. So node j can authenticate a message from node i and vice versa. Aggregator Aj and Ai establish pairwise key KAj,Ai. Monitoring node Mj and Ai also establish pairwise key KM,Ai as illustrated in Fig. 2. The scheme[7-8] are applied for establishing a pairwise key.

Each aggregator Au and nodes in its cluster are assumed to establish a group key Kgroup,u using scheme[9]. The group key is used for choosing the monitoring node and protecting confidentiality during sending data. The notations that are used in this paper are given in Table 1.

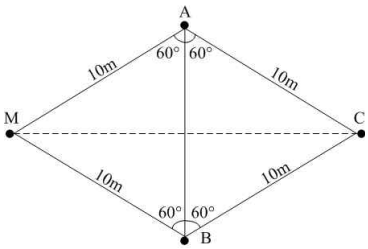

Fig. 2 a cluster in DAA

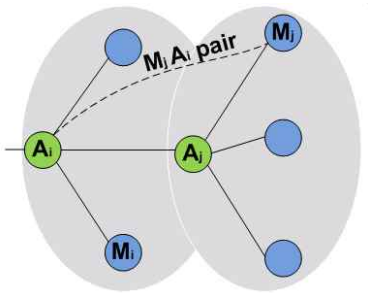

Fig. 3 Overlapping of 60° sextant clusters

IV. Proposed protocol

This section presents a monitoring based geographic routing protocol for filtering false aggregation data in wireless sensor networks. The proposed protocol provides secure data aggregation, data confidentiality and detecting false data.

Sensor nodes use geographic routing protocols [5-6] to set up clusters where a cluster consists of an aggregator and at least T sensor nodes. Clusters overlap each other as illustrated in Fig.3. After forming clusters, each cluster selects a monitoring node in order to overhear data, computes aggregation data Dagg as well as generates a MAC. A monitoring node will be randomly selected by all nodes in the cluster in order to prevent a compromised aggregator from affecting the selection of a monitoring node. An algorithm[1] is adopted for the selection of a monitoring node. Then the monitoring node makes a pair mate with a forward aggregator. As illustrated in a dash line in Fig. 2, monitoring node Mj in cluster j and forward aggregator Ai in cluster i form a Mj Ai pair mate.

Table 1. Summary of notations

Notation	Meaning
Aj	Current aggregator
Ai	Forward aggregator
M	Monitoring node
Ki,j	Key shared between node i and j
MACj,i(D)	Message Authentication Code of data D calculated with key Ki,j
Kgroup,j	Group key of cluster j
EK_ij(D)	Encryption of data D with key Ki,j
Dagg	Aggregation data

In data aggregation session, sensor nodes send encrypted data to their aggregator Aj. Aggregator Aj decrypts and aggregates them. Monitoring node Mj also aggregates data in its cluster. Note that sensor nodes in cluster j use key Kgroup,j to encrypt and decrypt data. After that, each aggregator Aj and monitoring node Mj generates MACj,i(Dagg) and MACM,i(Dagg), respectively. Monitoring node Mj sends MACM,i(Dagg) to aggregator Aj. Aggregator Aj sends EKgroup,i(Dagg) along with the concatenation of MACj,i(Dagg) and MACM,i(Dagg) to forward aggregator Ai. Aggregator Ai decrypts EKgroup,i(Dagg) to obtain plain Dagg and uses key Ki,j and

Ki,M to verify MACj,i(Dagg) and MACM,i(Dagg).

If MACj,i(Dagg) sent by Aj does not match with MACj,i(Dagg) computed by Ai or MACi,M(Dagg) sent by Mj does not match with MACi,M(Dagg) computed by Ai then this Dagg will be dropped because the verification fails. This implies that data aggregated by aggregator Aj and data monitored by monitoring node Mj are inconsistent. The proposed protocol for securing data and filtering false data can be found in Table 2.

V. Simulation and evaluation

To evaluate how efficiently detect false data and how much energy consumption is saved, this section can be divided into three parts: 1) network environment; 2) energy consumption for detecting false data and 3) comparison of our proposed protocol and related works in terms of security aspects and energy consumption.

1. Network environment

Since the previous false data detection techniques[2-4] do not address filtering false data and confidentiality, our work is compared with the DAA. The network environment is set up as follows. The base station is located at coordinate (0,0). The transmission range between two sensor nodes reaches a maximum of 20 meters (m). 200 sensor nodes are scattered over an area of 100 × 100 m2. As demonstrated in Section II, DAA requires a large transmission range. Therefore, let the sensor network of our work and DAA be divided into 40 and 20 clusters, or equally, there are 5 and 10 sensors in each cluster on average, respectively. Let the size of a message including IDs, a data value the and the concatenation of MACs be 1,000 bits. The initial energy budget at each sensor node is set at 0.5 J.

2. Energy consumption

The energy model of Heinzelman [10] is used to evaluate the energy consumption for transmitting a message E_{Tx} which is represented as the following equation,

$$s.(\delta+\theta.d^{q}) \qquad (1)$$

where s is the message size and δ (μJ/b) is the energy required to communicate one bit of information. The θ = 100 pJ/b/m is the coefficient for a distance-dependent term. The q = 2 is the exponent for the distance-dependent term, and d is the transmission distance.

Table 2. A protocol for securing data and filtering false data

Input: the current aggregator Aj, the forward aggregator Ai, nodes in cluster of Aj and Ai including monitoring nodes. Output: Any false data, that are injected during data aggregation are detected and dropped. 1: Sensor node in cluster j send data values which are encrypted using Kgroup,j to their aggregator Ai 2: When Aggregator Ai receives all data from sensor nodes in cluster j, it decrypts those data using Kgroup,j, aggregates those data (Dagg) and computes MACj,i (Dagg). 3: Monitoring node M in cluster j also aggregates data (Dagg) and computes MACM,i(Dagg). Then node M sends this MACM,i(Dagg) to aggregator Aj 4: Aggregator Aj sends encrypted data EKgroup,i(Dagg) along the concatenation of MACj,i(Dagg) and MACM,i (Dagg) to forward aggregator Ai 5: Aggregator Aj decrypts EKgroup,i(Dagg) using Kgroup,i to obtain plain aggregation data (Dagg) and then verifies both MACj,i(Dagg) and MACM,i(Dagg) using Ki,j and Ki,M , respectively. If the verification of MACK_j,i (Dagg) or MACK_M,i (Dagg) fails, Dagg will be dropped.

The energy in receiving a message of a node E_{Rx} is

$$s.\delta \qquad (2)$$

Total consumed energy of a cluster, Ecluster is

$$\sum_{i=1}^{m} E_{Tx} + \sum_{i=1}^{m} E_{Rx} \qquad (3)$$

where m is a average number of sensor nodes in a cluster. Total consumed energy of a sensor network, Etot is

$$N \times E_{cluster} \qquad (4)$$

where N is the total number of clusters. Since monitoring nodes (including other cluster members)

in DAA have different longer transmission ranges, the transmission range of sensor nodes will be averaged. DAA has the average transmission range equal to $10\sqrt{3}$ m. In our proposed protocol, a transmission range of sensor nodes in a 60^{o} sextant cluster is 10 m. Whether there is a false data injection attack or not, both DAA and our work have to perform monitoring false data every data aggregation session. To compare efficiency in terms of energy consumption, equation 4 is used to measure energy consumption between DAA and our work. Energy consumption of our work remains 64% of total energy while that of DAA runs out of energy. The network lifetime of our work is 283% longer when comparing with DAA as illustrated in Fig. 4

3. Discussion and comparison

Table 3 summarizes security aspects of each work. All the techniques provide data integrity that ensures a message has not been altered, either maliciously or accidentally, in transit. Therefore, data integrity becomes a minimal requirement for security services. For verifying data integrity, DAA, [2-3], [11] and our work use either pairwise keys or cluster keys to compute the MAC. While work[4] uses monitoring based on rules in IDS. In works [2], [3] and [4], rather than using encrypted data, sensor nodes send plain data to the base station via intermediate nodes. Monitoring nodes play an important role in detecting false data. However, the attacker can eavesdrop on communications. Both DAA and our work provide data integrity, data confidentiality and filtering false data. Therefore, DAA and our work provide more effective security than the others.

In addition to the security aspects, this section discusses energy consumption as well. In the works [2], [3], [4] and [11] since false data packets are detected at the base station in which all data packets including false data packets travel H hops on average, it results in consuming much energy in sensor nodes due to sending false data.

Table 6. Comparison of security aspects

work	data integrity	data confidentiality	filtering false data
[1]	Yes	Yes	Yes
[2]	Yes	No	No
[3]	Yes	No	No
[4]	Yes	No	No
[11]	Yes	No	No
ours	Yes	Yes	Yes

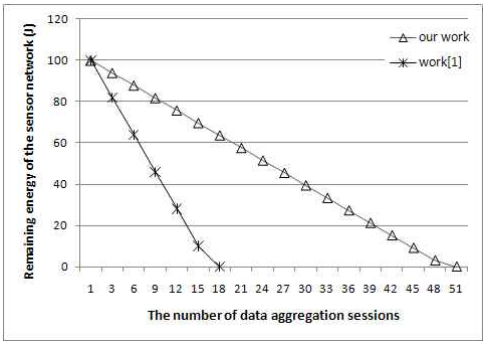

Fig. 4 Energy consumption

To reduce energy consumption in sending false data, our proposed protocol offers for filtering and dropping false data. Even DAA can filter false data, it requires sensors' large transmission range which requires much more energy. It is mainly because, unlike our work which uses a monitoring node in a 60^{o} sextant cluster, DAA uses large transmission area, with its optimal transmission range R, to detect false data . As a result, our simulation shows that 64% of energy remains in our novel approach while that of DAA runs out of energy. The network lifetime of our proposed protocol is 283% longer when comparing with DAA.

VI. Conclusion

This paper proposed an effective protocol for monitoring based secure data aggregation and filtering false data in wireless sensor networks. The proposed protocol allows higher security for data aggregation providing data confidentiality, and less

consumption for energy of the sensor network. Our simulation shows that energy consumption of our work remains 64% of total energy at the moment that of DAA runs out of energy. The network lifetime of our work is 283% longer when comparing with DAA[1].

References

[1] S. Ozdemir and H. Cam., "Integration of False Data Detection with Data Aggregation and Confidential Transmission in Wireless Sensor Networks," IEEE/ACM Transactions on Networking, Vol.18 No.3, pp. 736-749, 2010.

[2] A. Boonsongsrikul, K. Lhee and M. Hong, "Securing Data Aggregation against False Data Injection in Wireless Sensor Networks," Proceedings of the 12th International Conference on Advanced Communi cation Technology (ICACT'2010), pp. 29-34, 2010

[3] A. Boonsongsrikul, S. K. Park and S. H. Shin., "An Approach of False Data Identification Protocol for Minimum Communication Cost in Wireless Sensor Network," Journal of Korea Society of Computer and Information, vol. 16, No. 10, pp. 121-129, 2011.

[4] A. De Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz and H. C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, pp. 16-23, 2005

[5] B. Blum, T. He, S. Son, and J. Stankovic, "IGF: A state-free robust communication protocol for wireless sensor networks," Technical Report CS-2003-11, University of Virginia, Charlottesville, VA, 2003.

[6] A. D. Wood, L. Fang, J. Stankovic and T. He, "SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks," Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 35-48, 2006

[7] J. Deng and Y. S. Han, "Using MDS codes for the key establishment of wireless sensor networks," in LNCS 3794. Berlin, Germany: Springer-Verlag, 2005, pp. 732 - 744.

[8] Q. Dong and D. Liu, "Using auxiliary sensors for pairwise key establishment in WSN," in Proceedings of IFIP International Conference Networks, 2007, pp. 251 - 262.

[9] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yungand, "Perfectly-secure key distribution for dynamic conferences," Proceedings of Crypto, 1992, pp. 471 - 486.

[10] W. R. Heinzelman A. Ch and H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd Hawaii International Conference on System Sciences, pp. 3005 - 3014, 2000.

[11] A. Boonsongsrikul, K. Lhee and S. K. Park., "Monitoring-Based Secure Data Aggregation Protocol against a Compromised Aggregator ata AggregatSensor Networks," Journal of Korea Information Procegaing Society, vol. 18-c, No. 5, pp 303-316, 2011.

저 자 소 개

Anuparp Boonsongsrikul

1998 : Mahanakorn기술대학교 통신공학과 공학사.

2002 : Kasetsart대학교 전자공학과 공학석사.

현 재 : 아주대학교 정보통신공학과 박사과정

관심분야 : 센서 네트워크, Ad-hoc 네트워크, VANET, IC 디자인 등

Email : anuparp@ajou.ac.kr

박 승 규

1974 : 서울대학교 응용수학과 학사

1976 : 한국과학원(KAIST) 전산학과 석사

1982 : Institut National Polytechnique de Grenoble 전산학과 박사

1976~1992 : KIST, KIET, ETRI 선임/책임연구원

1992~현재 : 아주대학교 정보 및 컴퓨터공학부 교수

관심분야 : 임베디드 테스팅, 자가 컴퓨팅/치료 시스템, 차세대 컴퓨터 구조 등

Email : sparky@ajou.ac.kr

신 승 훈

2000 : 아주대학교 정보컴퓨터공학부 공학사

2002 : 아주대학교 정보통신공학과 공학석사

2011 : 아주대학교 정보통신공학과 공학박사

2011 : 아주대학교 정보컴퓨터공학부 특임교원

관심분야 : 소프트웨어 테스트 자동화, 멀티미디어 데이터 전송 정책 등

Email : sihnsh@ajou.ac.kr