International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:6, 2008

Simulation using the Recursive Method in USN

Tae Kyung Kim, and Hee Suk Seo

***Abstract*—**Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects forged reports into the network through compromised nodes, with the goal of deceiving the base station or depleting the resources of forwarding nodes. Several research solutions have been recently proposed to detect and drop such forged reports during the forwarding process. Each design can provide the equivalent resilience in terms of node compromising. However, their energy consumption characteristics differ from each other. Thus, employing only a single filtering scheme for a network is not a recommendable strategy in terms of energy saving. It's very important the threshold determination for message authentication to identify. We propose the recursive contract net protocols which less energy level of terminal node in wireless sensor network.

***Keywords*—**Data filtering, recursive CNP, simulation.

I. Introduction

SENSOR networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects forged reports into the network through compromised nodes, with the goal of deceiving the base station or depleting the resources of forwarding nodes. Sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities [3]. Sensor networks are expected to interact with the physical world at an unprecedented level of universality, and enable various new applications [4]. In many applications, sensor nodes are deployed in open environments, and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys [5]. Forged sensing reports can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in battery powered networks. Several research solutions have been recently proposed to detect and drop such forged reports during the forwarding process. Each design can provide the equivalent resilience in terms of node compromising. However, their energy consumption characteristics differ from each other. Thus, employing only a single filtering scheme for a network is not a recommendable strategy in terms of energy saving. It's very important the threshold determination for message authentication to identify. We propose the recursive contract net protocols which less energy level of terminal node in wireless sensor network.

H. S. Seo is with the Korea University of Technology and Education, Byungcheon, Chungnam 330-708 Korea (corresponding author to provide phone: +82-41-1495; fax: +82-41-1462; e-mail: histone@kut.ac.kr).

T. K. Kim is with the Seoul Theological University, Bucheon-City, Kyonggi 422-742 Korea (e-mail: tkkim@ stu.ac.kr).

II. Background

A. Commutative Cipher Based En-route Filtering Overview

In [6], Yang and Lu proposed the commutative cipher based en-route filtering scheme (CCEF) to defend against false data injection attacks without symmetric key sharing among sensor nodes. A commutative cipher is used to endorse and verify sensing reports. A commutative cipher *CE* satisfies the following property: for any message M and any two keys K_1 and K_2,

$$CE(CE(M,K_1),K_2) = CE(CE(M,K_2),K_1) \quad (1)$$

The monitoring capability in CCEF is protected by the secrets shared between the sensor nodes and the base station, while the en-route filtering capability is achieved through a partial proof of the secret association [6]. As a result, CCEF can provide much stronger security protection against node compromising than the symmetric cryptography based security solutions.

In CCEF, every node has a unique ID and is preloaded with a unique key, which is shared only with the base station. In the operational phase, the sensor nodes are tasked by the base station through queries. For each session, the base prepares two keys K_s and K_w:

$$CE(M,K_w) = CE^{-1}(M,K_s), \quad (2)$$

where *CE* and CE^{-1} are the encryption and decryption algorithm of a commutative cipher, respectively. Then, the base station randomly selects one sensor node at the location of interest as a cluster head and sends a query toward the cluster head. A unique query ID *QID*, the cluster head's ID *CID*, K_s encrypted by the cluster head's key, and K_w as plaintext are included in the query. Each intermediate node stores the *QID* and K_w for future verification purpose. When the cluster head receives the query, it decrypts the K_s and then forwards the query to its local neighbors (Fig. 2(a)). Thus, after the query propagation, every intermediate node has *QID* and K_w, and the cluster head has *QID* and K_s (Fig. 2(b)). Then, the cluster head generates a sensing report. Each sensing report is endorsed by two MACs. One is generated by the cluster head using K_s. The other is generated by its neighbor nodes using their keys. A report is forwarded toward the base station along the reversed path as the query traverses. Every forwarding node can verify the report using K_w:

$$CE(CE(R,K_s),K_w) = R \quad (3)$$

CCEF uses a probabilistic approach in which a forwarding node verifies a report with a verification probability P since the

commutative cipher computation is quite heavy (Fig. 2(c)). *P* is calculated by:

$$P = \frac{1}{\alpha h}, \tag{4}$$

where α is a security parameter and h is the number of hops from the cluster head to the base station. Finally, the report is verified by the base station.

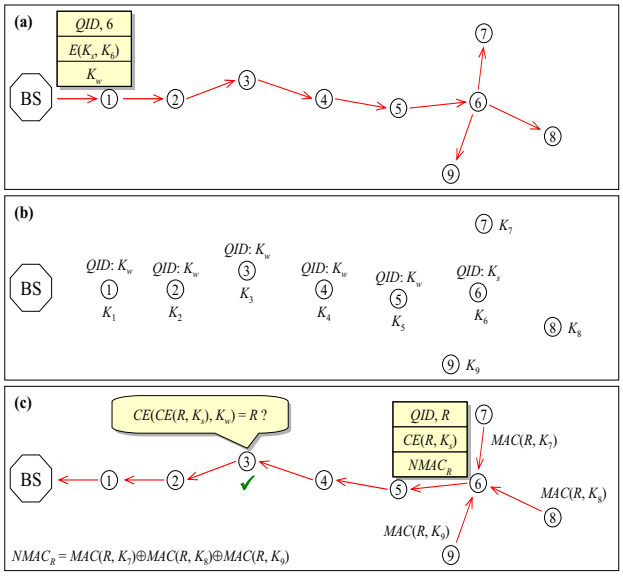

Fig. 1 The overview of CCEF

B. DEVS and SES

The DEVS formalism is a theoretically well-grounded means of expressing modular discrete event simulation models developed by Zeigler [11,12]. A DEVS is a structure:

$$M = < X, S, Y, \delta int, \delta ext, \lambda, ta >$$

Where X : the set of input event types,
S : the sequential state set,
Y : the set of external event types generated as output,
δ int : S→ S, the internal transition function,
δ ext : Q×X→ S, the external transition function,
$Q = \{(s,e) \mid s \in S, 0 \leq e \leq ta(s)\}$
λ : S→ Y , the output function,
ta : S→ R+0, ∞ , the time advanced function,
R+0, ∞ is a real number set except a negative number.

X means the set of events that occur outside the system. Y means the set of output variables. S means the cross product of definition areas of state variables and s ($s \in S$) means the sequential snap shot of system according to time progress. ta(s) is defined as the time allowed to be at the state s unless system doesn't get external events. δ int is defined as the function that explains the change of the state of model according to time progress when there are no external events. δ ext is defined as the function that represents the change of the state of model by the events occurred in the outside of the system. λ is defined as the output of the system in the state s. The DEVS environment supports building models in a hierarchical and modular manner, in which the term "modular" means the description of a model in such a way that is has recognized input and output ports through which all interaction with the external world is mediated. This property enables hierarchical construction of models so that the complex network security models can be easily developed.

The SES (System Entity Structure) [13] directs the synthesis of models from components in the model base. The SES is a knowledge representation scheme that combines the decomposition, taxonomic, and coupling relationships.

The entities of the SES refer to conceptual components of reality for which models may reside in the model base. Also associated with entities are slots for attribute knowledge representation. An entity may have several aspects, each denoting a representation. An entity may also have several specializations, each representing a classification of the possible variants of the entity.

III. Proposed Model

To allow effective coordination and control of tasks, CNP allocates agents to the tasks. In this approach, agents coordinate through contracts to accomplish a goal. Contracting involves an exchange of information among agents, an evaluation of the information and a final agreement based on mutual selection. In other words, CNP selects the best agent to serve jobs by bidding and then the selected agent performs the jobs.

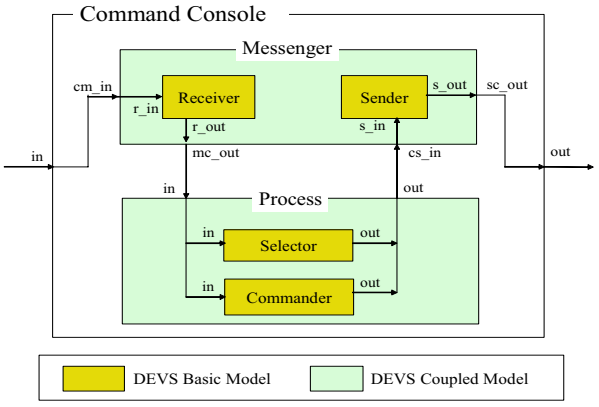

Fig. 2 Structure of Command Console model

The contract net protocol was originally proposed as a tool for communication and control in a distributed problem solver. It provides a mechanism for agents to communicate and negotiate to solve a distributed problem via contracts. A contract is a set of tasks to be accomplished. Agents announce

tasks that they need, make bids to perform tasks announced by other agents. And then agents evaluate the bids and award contracts. Contract net protocol is essentially a collection of nodes which cooperate to resolve a problem [12].

A. Recursive CNP

The survivability of each node is very import problem in the wireless sensor network. The survivability of each node plays a definite role in the WSN. We proposed the recursive contract net protocol for effective USN network operation as BS, GH(Group Header), CH(Cluster Header). The CNP, the methodology for efficient integration of computer systems on heterogeneous environment such as distributed systems, is essentially a collection of agents which cooperate to resolve a problem.

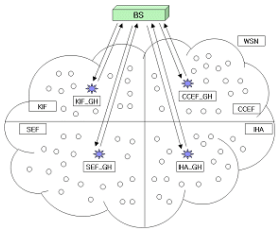

Fig. 3 CNP of BS

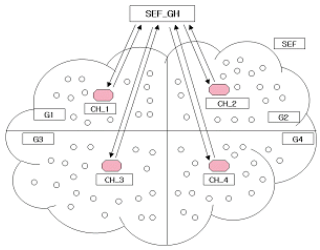

Fig. 4 CNP of GH

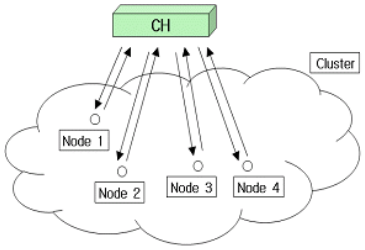

Fig. 5 CNP of CH

If simulation starts up and packets come into the internal network, Command Console sends bid message to all IDS agent. After receiving bid message, each agent makes bid and sends bid_data message. Command Console selects IDS agent to detect an intrusion by selection algorithm with bid_data and sends award message to the selected IDS agent. After receiving award message, the selected agent preparesfor the detection of intrusion and waits for packet_data message. Command Console copies packet data to packet_data message and sends it. The selected IDS agent detects an intrusion from packet_data. If the state of Detector model becomes Failed state, agent sends announcement message to Command Console and after receiving it Command Console repeats the coordination cycle.

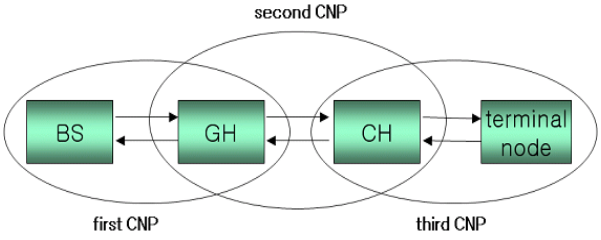

Fig. 6 Recursive CNP

If the number of compromised nodes exceeds the number of cluster nodes, the IHA may be inefficient or even useless [9]. For example, the IHA cannot filter false reports injected by five colluding compromised nodes when the threshold value is smaller than 5. Under this situation, we may as well disable the en-route filtering, i.e., set a security threshold value to 0. So, we have to determine a security threshold value based on the number of cluster nodes and the number of compromised nodes. The energy is the most important resource that should be considered in sensor networks. Generally, sensor nodes are limited in power and irreplaceable since these nodes have limited capacity and are unattended [15]. Therefore, we also have to determine a threshold value based on the energy level of nodes.

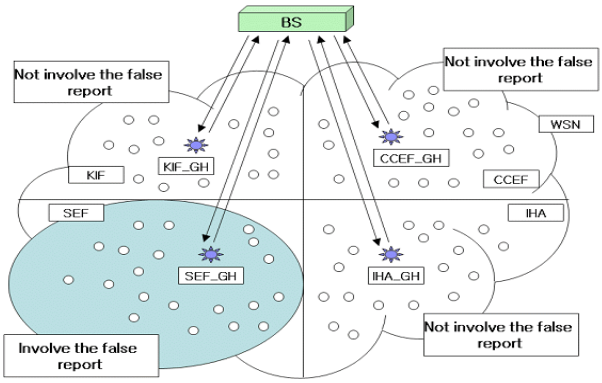

Fig. 7 First CNP

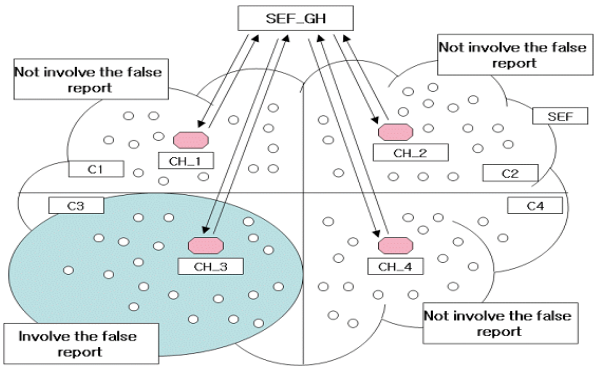

Fig. 8 Second CNP

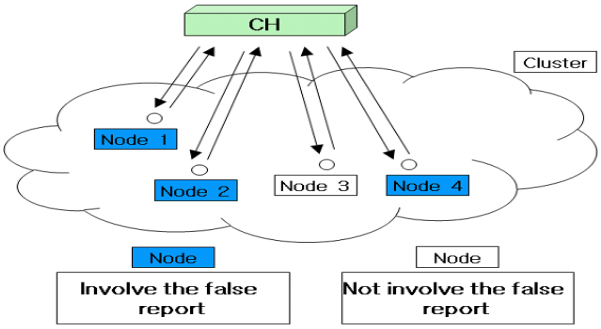

Fig. 9 Third CNP

IV. Conclusion

Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects forged reports into the network through compromised nodes, with the goal of deceiving the base station or depleting the resources of forwarding nodes. Several research solutions have been recently proposed to detect and drop such forged reports during the forwarding process. Each design can provide the equivalent resilience in terms of node compromising.

In this paper, we proposed a fuzzy logic for the adaptive security threshold determining in the interleaved authentication-based sensor networks. For the path to each cluster, the fuzzy logic determines the threshold value by considering the number of cluster nodes, the number of compromised nodes, and the energy level of nodes. The fuzzy-based threshold determining can conserve energy, while it provides sufficient resilience. The effectiveness of the proposed method was shown with the simulation result.

The proposed method can be applied to the en-route filtering schemes that needs to choose a security threshold value. Our future research will be focused on optimizing the proposed method and applying it to various en-route filtering schemes.

References

[1] Wang, G., Zhang, W., Cao, G., Porta, T.L.: On Supporting Distributed Collaboration in Sensor Networks. In Proc. of MILCOM (2003) 752-757.
[2] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A Survey. Comput Netw 38(4) (2002) 393-422.
[3] Ye, F., Luo, H., Lu, S.: Statistical En-Route Filtering of Injected False Data in Sensor Networks. IEEE J. Sel. Area Comm. 23(4) (2005) 839-850.
[4] Przydatek, B., Song, D., Perrig, A.: SIA: Secure Information Aggregation in Sensor Networks. In Proc. of SenSys (2003) 255-265.
[5] Yang, H, Lu, S.: Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks. In Proc. of VTC (2003) 1223-1227.
[6] Zhu, S., Setia, S., Jajodia, S., Ning, P.: An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks. In Proc. of S&P (2004) 259-271.
[7] Zhang, Y., Yang, J., Vu, H.T.: The Interleaved Authentication for Filtering False Reports in Multipath Routing based Sensor Networks. In Proc. of IPDPS (2006).
[8] Ganesan, D., Govindan, R., Shenker, S., Estrin, D.: Highly-resilient, Energy-efficient Multipath Routing in Wireless Sensor Networks. In Proc. of SIGMOBILE (2001) 251-254.
[9] Zhang, W., Cao, G.: Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach. In Proc. of INFOCOM (2005) 503-514.
[10] B. P. Zeigler, H. Praehofer and T.G. Kim, Theory of Modeling and Simulation, Academic Press, 2000.
[11] S.H. Chi and T.H. Cho, "Fuzzy Logic based Propagation Limiting Method for Message Routing in Wireless Sensor Networks," Lect. Notes Comput. Sc., vol.3983, pp.58-64, May 2006.
[12] Yu, Z., Guan, Y., "A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks," In Proc. Of SenSys, pp. 294-295, 2005.
[13] Zhang, Y., Liu, W., Lou, W., Fang, Y., "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," IEEE J. Sel. Area Comm. Vol.24, pp. 247-260, 2006
[14] F. Li and J. Wu, "A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," Proc. of IWCMC, pp. 27-32, Jul. 2006.
[15] Seo, Hee Suk, "Network security agent DEVS simulation modeling," Simulation Modelling Practice and Theory, Elsevier Science B.V., Vol. 14, Issues , pp. 481-492, Oct. 2005.