Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/1399
DOI URL: http://dx.doi.org/10.21474/IJAR01/1399
ISSN NO. 2320-5407

RESEARCH ARTICLE

A CORRELATION ANALYSIS OF THE MAC LENGTH IN STATISTICAL EN-ROUTE FILTERING BASED WSNS.

Jung-Sub Ahn[1] and[*]Tae-Ho Cho[2].

1. College of Information and Communication Engineering, Sungkyunkwan University, Korea.
2. College of Software, Sungkyunkwan University, Korea.

Manuscript Info

Manuscript History

Received: 13 June 2016
Final Accepted: 18 July 2016
Published: August 2016

Key words:-
Wireless sensor network, statistical en-routfiltering , false report injection attack

Abstract

Wireless sensor networks have various applications including in military, medical and industrial fields. Wireless sensor networks consist of a large numbers of sensor nodes, which are deployed in large fields and open environments. Therefore, sensor nodes are vulnerable to physical attacks and are exposed to false report attack. This attack cause depletion of the sensor node energy. Statistical en-route filtering was proposed to improve energy efficiency and detection power before injected false reports arrive at the base station. The Message Authentication Code (MAC) length of Statistical en-route Filtering affects the energy efficiency and detection ratio. If sensor nodes have a high MAC length in an area with a low attack ratio, the energy efficiency is lower. In this paper, we show energy consumption according to attack ratio looking for optimal MAC length in simulation using discrete event system specification based on statistical en-route filtering.

Introduction:-

Wireless Sensor Networks (WSNs) consist of sensor nodes that detect events and forward reports, along with a base station node (BS) that collects the event information from the sensor nodes [1, 2]. WSNs consist of a large number of sensor nodes with sensing, wireless communications capability. Therefore, they should have low cost and include fault tolerance. Sensor nodes have limited battery capacity, computation and storage capacity. WSNs are vulnerable to physical attacks because sensor nodes are deployed in an open environment [3]. An attacker can gain access to a node, and it is possible to obtain sensitive information such as secret keys. An attacker can cause a false report injection attack using the collected information. A false report injection attack sends false reports to the BS, resulting in false event alarms and possibly network paralysis [4]. Ye et al. proposed the Statistical en-route filtering (SEF) scheme to solve this problem [4]. SEF is a technique that detects and drops false reports through the co-operative communication of sensor nodes. Security and Energy consumption are determined by SEF according to the MAC length. In this paper, our aim is to extract the optimal MAC length through simulation including attack ratio, and node density.

Related works:-

This section reviews false report injection attacks, the concept of SEF, and the DEVS simulation procedure, which are required to understand this paper.

Corresponding Author:-Tae-Ho Cho.
Address:-College of Software, Sungkyunkwan University, Korea.

False Report Injection Attack:-

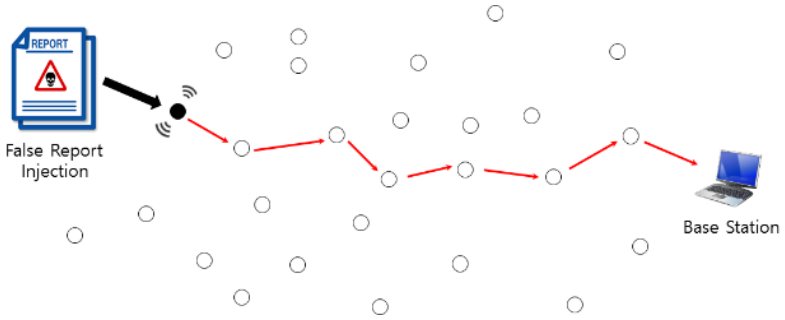

Fig. 1:- False report injection attack.

The false injection attack is shown in Fig. 1. A false report injection attack generates false reports including false event information and inject them into the network. A false report injection attack causes false event alarms and unnecessary energy consumption at the BS. Especially, if an attack occurs repeatedly, it can result in rapid energy exhaustion of the sensor nodes.

Static En-route Filtering:-

SEF is a scheme used to eliminate false report injection attacks on WSN by detecting them early. When an event occurs, the report is stochastically verified by a center-of-stimulus (Cos) input key with a threshold value to report. Threshold is number of MACs in a report. The report mid-verification should detect the wrong report early to prevent an unnecessary energy use. SEF consists of three phases: the key division phase, the generating report and mid-filtering phase and the BS verification phase. The user sets the threshold value and error bound for the sensor nodes before they are placed at the target area. Each node shares the key sets for the partition units assigned randomly at the global key pool. Fig. 2 shows the process for key distribution.

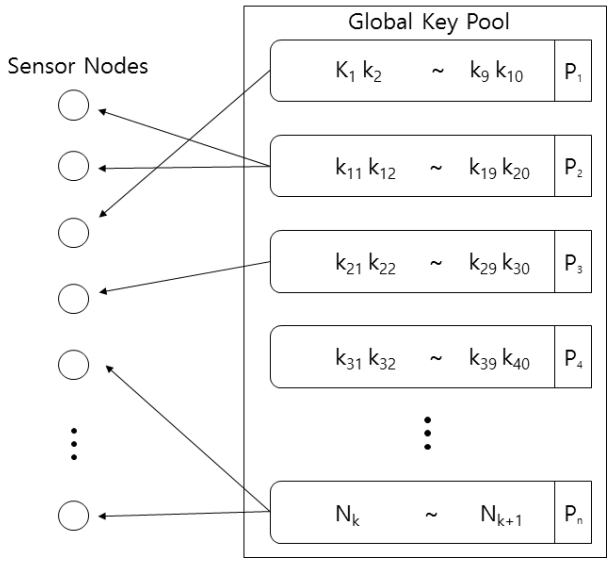

Fig. 2:- Key Distribution.

Randomly deployed sensor nodes detect the event and the node with the strongest signal is chosen as the Cos node. The Cos node sends a broadcast signal to find neighboring nodes with the same event signal value. The neighboring nodes that receive the signal generate a MAC using their own keys distributed previously and send the keys to the Cos node. Fig. 3 shows the report generation process at the Cos node using the collected MACs.

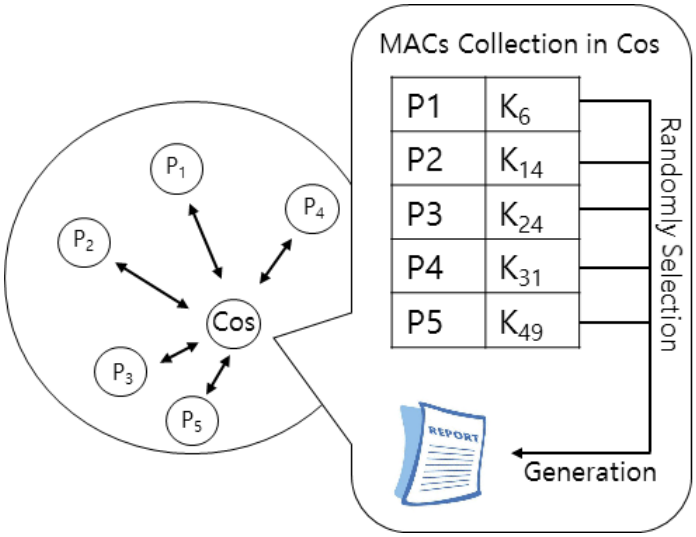

Fig. 3:- Report Generation.

The event report is transmitted to the Cos node by the multi-hop routing scheme [5]. A higher threshold value increases the probability of detecting a false report and makes it harder for attackers to generate false reports. If a node receives the event report en-route to BS, they node verifies the key for the report. Fig. 4 shows the en-route filtering.

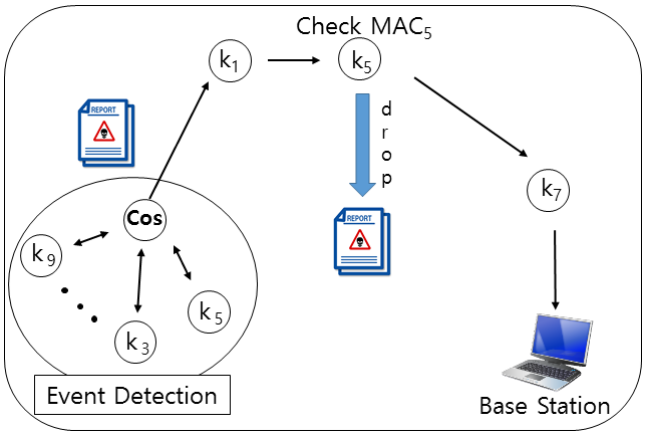

Fig. 4:-En-route Filtering.

Forwarding nodes generate new event reports using their own keys and verify the received event report using the generated event report in advance. If the generated report equals the received report, it is transmitted to the next hop node. Otherwise, the node drops the received report. Finally, BS receives the report and verifies all of the MACs using the global key pool [3].

DEVS Simulation:-

The DEVS formalism proposed by Zeigler has the value of state and executes the simulation by moving dynamically [6, 7]. DEVS is a discrete event model with finite discrete values. It is used to derive an imaginary result when a specific situation occurs. DEVS has a hierarchical structure and time value where more realistic simulation is possible to extract precise data. DEVS has the following advantages.

- Reusability of the model is easy.
- There is a port and a function each for the external/internal event.
- DEVS has next event schedule execution time value and status value per model.
- There is time value that controls the timing of transition.

DEVS is composed of a coupling model combined with the atomic model. The atomic model is composed as follows.

AM = < X, S, Y, t_a, δ_{ext}, δ_{int}, λ >
X: input events set;
S: sequential states set;
Y: output events set;
t_a: time advance function;
δ_{ext}: external transition function;
δ_{int}: internal transition function;
λ : output function;

X is the set that identifies the event input, S is the set that identifies the state of the model, and Y is the set of the event output. ta is the time value in S. δ_{ext} is the external transition function for whether to maintain a certain state when X input is entered. δ_{int} is the internal transition function that changes internally with no relations to the external input. λ is the output function.
The coupling model connects the atomic models and creates a large system. The coupling model is composed as follows.

CM = < X, Y, {M_i}, IC, EIC, EOC, Select >
X: input events set;
Y: output events set;
M_i: sub-components set;
IC: internal couplings;
EIC: external input couplings;
EOC: external output couplings;
Select: tie-breaking selector function;

M is the name set of the composed model. IC connects the internal models, while EIC and EOC show the relationship between models. Select grant the priority to decide on which model to execute among the available models.

Assumption:-
The WSN used for simulation consists of the Cos, sensor nodes and BS. This simulation is based on the Cluster system [8]. The WSN model is applied to MICA2. If an event is detected, a report is sent to the BS. Each node formulates an automatically routed path by cooperative communication with other nodes. Each node has the index number for the key, which is used to obtain check verifications.

Overview:-
The threshold value in SEF has an influence on the energy efficiency. Our purpose is to extract the optimal threshold value using various parameters. Simulations were performed with CH, MB and BS models. The CH model represents the Cos node, the MB model represents the neighboring nodes and BS model is for the BS, which receives reports.

DEVS Models :-

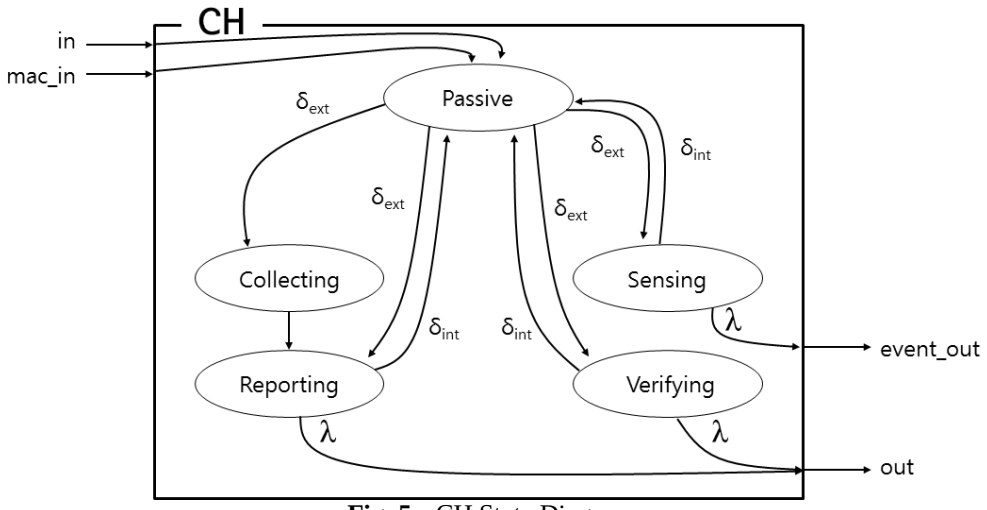

Fig. 5:- CH State Diagram.

Fig. 5 is the state diagram for the CH model. The CH model has 5 possible states including the passive state, which is the standby state. The CH atomic model has two input ports of the in-port and mac-in-port, as well as two output ports, the out and event_out ports. When in a passive state, the model remains in standby until a signal is received. When a message arrives at the input port, the received message state is analyzed and the model changes to a sensing, verifying, reporting, or collecting state. The sensing state is the stage for delivering event messages that have occurred in neighboring nodes. And the collecting state is for collecting the MAC of neighboring nodes. Reporting is the stage for generating reports using the collected MACs and delivering them to the out port, while verifying is the stage for receiving and verifying the report.

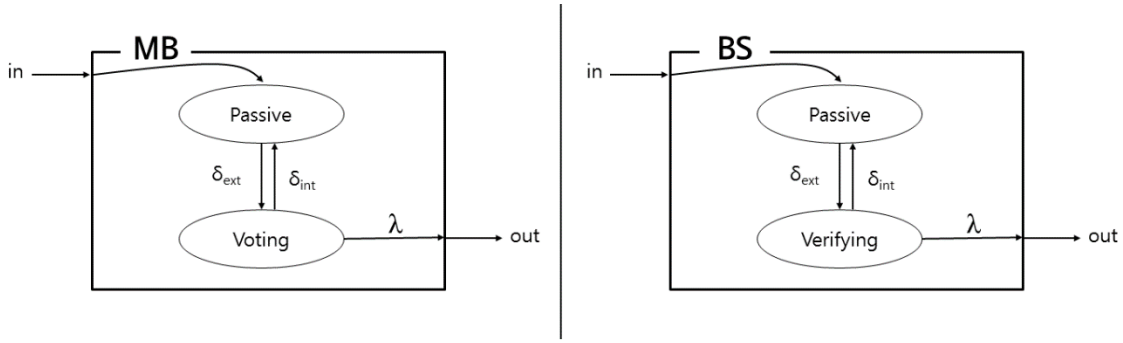

Fig. 6:- MB and BS State Diagram.

Fig. 6 is the state diagram for the MB and BS Models. MB has two states. A MAC is generated when a message is received through the in port and the voting state is for delivering the MAC message through the Cos node. The BS model also has two states. When a report comes in through the in port, the state is changed to Verifying to verify the authenticity of the report. In the Verifying state phase, the integrity of MAC of the report is verified using the global key pool.

Structure of Model:-

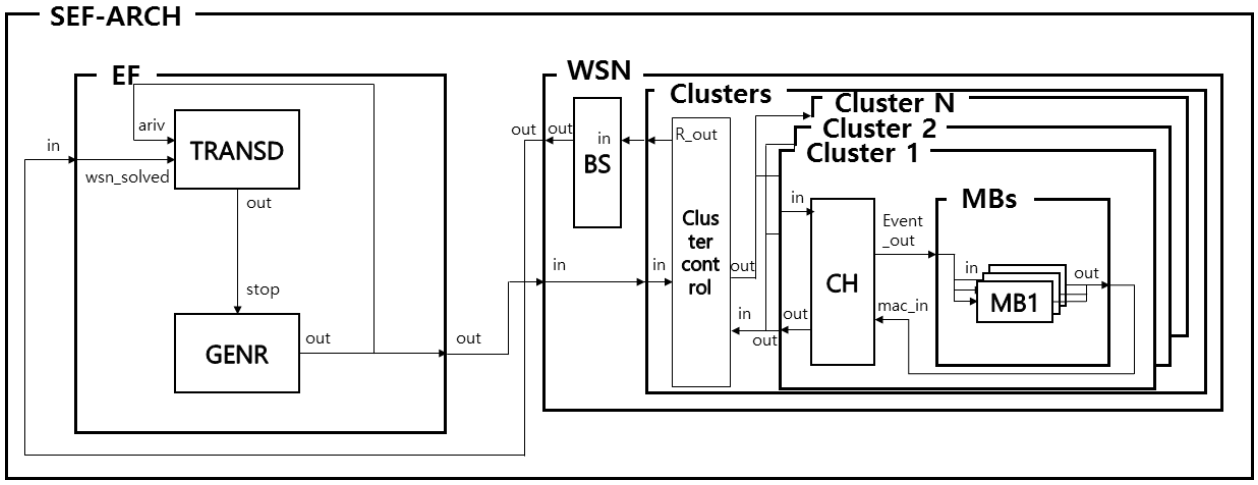

Fig. 7:- Atomic and Coupling Model.

Fig. 7 shows the composition of the simulation. The EF model and the WSN model are combined in the SEF-ARCH. WSN is composed of one BS and several cluster models. One cluster is divided into a CH model and various MBs models. When an event occurs, the message is received by the CH node through the in port and delivered to the MB model, which represents the surrounding neighboring nodes, through the event_out port. In MB, the MAC is created again through the CH model and then delivered. In the CH model, the report is made and delivered through the out port to the BS.

Experiments result:-

In this section, the performance of SEF according to threshold value and attack ratio is compared through simulation. The virtual sensor field size is 1,000×1,000m^2 and deployed into 1,000 nodes. Each node is consumed with 16.25μJ energy when transmitting data and 12.5μJ when receiving data. When generating MAC, 15μJ is consumed, and 75μJ is consumed in the forwarding node verification. The size of the report is 36 bytes and one MAC is assumed to be 1 bite. The global key pool has 10 partitions, and each partition has 10 keys. Event can occur randomly in all nodes, and a total of 200 events occur.

Fig. 8:- Energy Consumption versus False traffic ratio.

Fig. 8 shows the energy consumption according to attack ratio and threshold value. Fig. 8 is composed of 100 CH nodes and each CH node is composed of 9 MB nodes. As a result, the false traffic ratio is 75% and shows that around 300mJ of energy is consumed in contrast to when the threshold value is 3. On the other hand, when the attach ratio is 25%, it shows that the least energy is consumed when the threshold value is 3.

Conclusion:-

The WSN is composed of nodes that are low cost and have limited processing ability, limited storage ability, and limited battery performance. When a false report insertion attack occurs, the node's energy is reduced. To address this issue, proposed the Statistical En-route Filtering scheme. The SEF scheme has different forwarding node verification rates and energy consumption rates according to the threshold value. In this paper, we simulated the energy consumption according to the attack rate, density, and threshold value. As a result, the entire network lifespan increases by setting the threshold value to high value when the false traffic ratio is high in WSN. For future research, various issues that may occur in the established system as well as the decision technique for selecting the appropriate threshold value according to various environments should be identified and resolved.

Acknowledgements:-

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484)

References:-

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114, 2002.
2. J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, pp. 2292-2330, 2008.
3. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, vol. 1, pp. 293-315, 2003.
4. F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 23, pp. 839-850, 2005.
5. J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," Wireless Communications, IEEE, vol. 11, pp. 6-28, 2004.
6. B. P. Zeigler, G. Ball, H. Cho, J. Lee and H. Sarjoughian, "The DEVS/HLA Distributed Simulation Environment And Its Support for Predictive Filtering," AI and Simulation Group Department of Electrical and Computer Engineering University of Arizona, Tucson, Arizona, September, 1998.
7. B. P. Zeigler, "DEVS theory of quantized systems," Advanced Simulation Technology Thrust DARPA Contract, 1998.
8. D. Ganesan, A. Cerpa, W. Ye, Y. Yu, J. Zhao and D. Estrin, "Networking issues in wireless sensor networks," Journal of Parallel and Distributed Computing, vol. 64, pp. 799-814, 2004.