Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/1377
DOI URL: http://dx.doi.org/10.21474/IJAR01/1377
ISSN NO. 2320-5407

RESEARCH ARTICLE

Detection of Compromised Nodes using Modeling and Simulation for Statistical En-route Filtering based Wireless Sensor Networks.

Su Man Nam[1] and *Tae Ho Cho[2].

1. College of Information and Communication Engineering, Sungkyunkwan University, Suwon 16419, Republic of Korea.
2. College of Software, Sungkyunkwan University, Suwon 16419, Republic of Korea.

Manuscript Info

Manuscript History

Received: 10 June 2016
Final Accepted: 13 July 2016
Published: August 2016

Key words:-
Wireless sensor networks,
En-route filtering schemes,
Modeling and simulation,
False report injection attacks

Abstract

Wireless sensor networks are subject to potential threats since sensor nodes are energy-constrained and are deployed in open-collaborative environments. The nodes are easily compromised by adversaries to generate false reports, called false report injection attacks. The false reports cause unnecessary energy consumption in intermediate nodes and cause false alarms in the sink node. To address the attacks, statistical en-route filtering detects the false report in intermediate nodes. Even though the scheme detects the false report, it is difficult to find the compromised nodes. In this paper, we show how the previously proposed context aware architecture can be exploited to detect the compromised nodes within the SEFbased WSN.The experimental results indicate that the proposed models detect the compromised nodes within a specific time.

Introduction:-

Wireless sensor networks (WSNs) are being used in numerous applications such as environmental and habitat monitoring, and surveillance and tracking for military applications [1-3]. The sensor network consists of a number of sensor nodes and a sink node in a sensor field [4]. The sensor node conducts data collection, data processing and control, and data forwarding in wireless communication. The sink node collects data from the sensor nodes, analyzes the data, and provides information to users. The sensor network is subject to potential threats because the sensors are energy-constrained and are deployed in open-collaborative environments.

As shown in Figure 1, a compromised node can inject false reports into the sensor network, called false report injection attacks [5, 6]. The false report not only consumes unnecessary energy in intermediate nodes but also causes a false alarm in the sink node. In addition, the sensor network shortens its lifetime via the false report.

Corresponding Author:-Tae Ho Cho.
Address:-College of Software, Sungkyunkwan University, Suwon 16419, Republic of Korea.

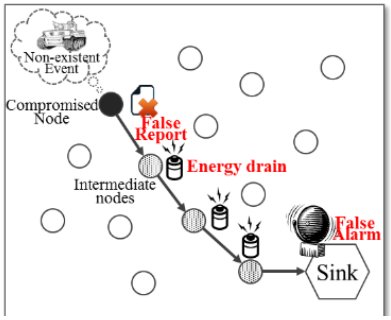

Figure 1:-False report injection attacks

To deal with false report injection attacks, statistical en-route filtering (SEF) [5] was proposed through the verification of message authentication codes (MACs) in a report. When an event occurs, the source node collects MACs from its neighbors and generates a report with the collected MACs. Intermediate nodes of the source verify the MACs when their keys match key indexes of the MACs. When an intermediate node detects a false MAC, it immediately filters out the report. Although SEF effectively detects false MACs against the false report injection attack, it is difficult to find compromised nodes in the sensor field because they can fabricate packet data such as the source address.The scheme proposed in [7] detects the compromised nodes in order to analyze data in a context aware architecture.

In this paper, we demonstrates how the previously proposed context aware architecture can be exploited to detect the compromised nodes within the SEF based WSN. The simulation model is shown for detecting compromised nodes in a SEF-based WSN by applying the architecture proposed in [7]. In addition, the model receives temporal data as described in [7]. This model has two subcomponent models (ANODE and CNTR) for analyzing the data in order to effectively detect the compromised nodes.

This paper is organized as follows. In Section 2, we describe the background and motivation of the proposal. Section 3 introduces our proposed method in detail, and Section 4 provides the analysis and experimental results. Finally, the conclusions and future work are discussed in Section 5.

Background:-

Statistical En-route Filtering (SEF):-

SEF is an en-route filtering scheme of the sensor network. This method filters out false reports through MAC verification in intermediate nodes while forwarding the reports. SEF consists of three phases: (1) key assignment and report generation, (2) en-route filtering, and (3) sink verification. In key assignment and report generation, the sink node has a pre-generated global key pool, divided into n non-overlapping partitions. Each partition has m keys, and each key has a unique key index.

The sink has a global key pool with n partitions (each partition has 10 keys). Before sensor nodes are deployed in a sensor field, the sink node randomly assigns keys from one of the n partitions. After deployment, one of the detecting nodes is elected as the center-of-stimulus (CoS) node as a real event occurs. The CoS node broadcasts event data $\{L_E, t, E\}$, where L_E is the location of the event, t is the time of detection, and E is the type of event [5], to neighboring nodes, and collects MACs from the neighbors. When an event is generated near the CoS node, the CoS node broadcasts event data to its neighbors. The neighboring nodes generate each MAC and submit the MAC and one of the key indexes. The CoS node then collects the MACs from them and randomly selects T MACs to attach them in a report without partition duplication. In en-route filtering, after the CoS forwards the generated report, the intermediate nodes verify the report if their keys match the key indexes of the MACs. When the intermediate node detects a false MAC in the report, it immediately drops the report.In sink verification, the sink node receives the false report from a CoS node, and the sink verifies all of the MACs in the report using the global key pool. When the report is normal, after verifying the MACs, the sink node provides the report information to users. On the other hand, if a false MAC is detected, the report is dropped.

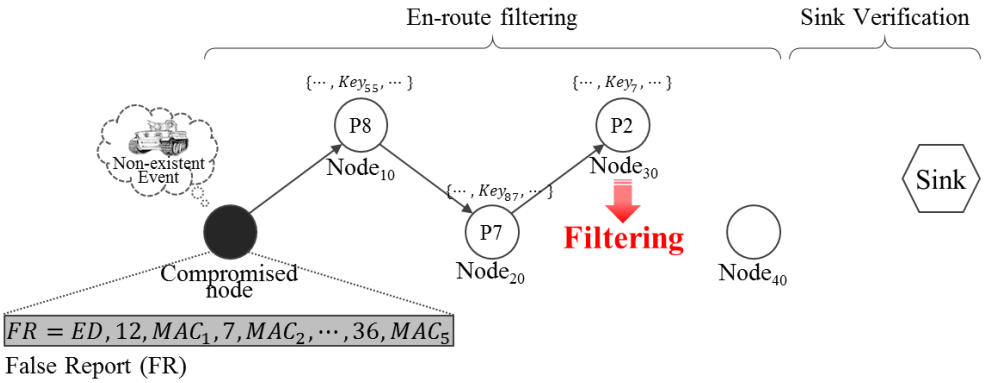

Figure 2:-An example of false report detection

Figure 2 shows an example of false report detection generated from a compromised node. As shown in Figure 3, the compromised node generated the false report using captured keys against the false report injection attack. When $Node_{10}$ receives the false report, $Node_{10}$ forwards the report to the next node without the MAC verification because it has matching keys. $Node_{20}$ also forwards it to $Node_{30}$. When the report arrives at $Node_{30}$, the node filters out the false report because a false MAC_2 is detected by using Key_7. Thus, SEF detects false reports through MAC verification in intermediate nodes against the false report injection attacks.

Context Aware Architecture for probabilistic voting-based filtering scheme:-
In [7], this method finds the adversary nodes injecting false data using in a context awareness-based architecture for a probabilistic voting-based filtering scheme (PVFS). In the method, to collect all of packets in the sensor field, it uses additional nodes to forward them to the architecture.

The method consists of four phases: (1) initialization and key assignment, (2) report generation, (3) en-route filtering, and (4) data verification. In the phase initialization and key assignment, the sink assigns keys to each node, and the node selects its verification nodes based on its distance. In the phase report generation, when a real event occurs, a source node generates a report including the collected MACs to forward it to the sink. In the en-route filtering, the selected verification nodes verify the MACs of the report using their keys. Lastly, as the packets are transmitted to the next node, the method collects all of packets and analyzes them based on its history.

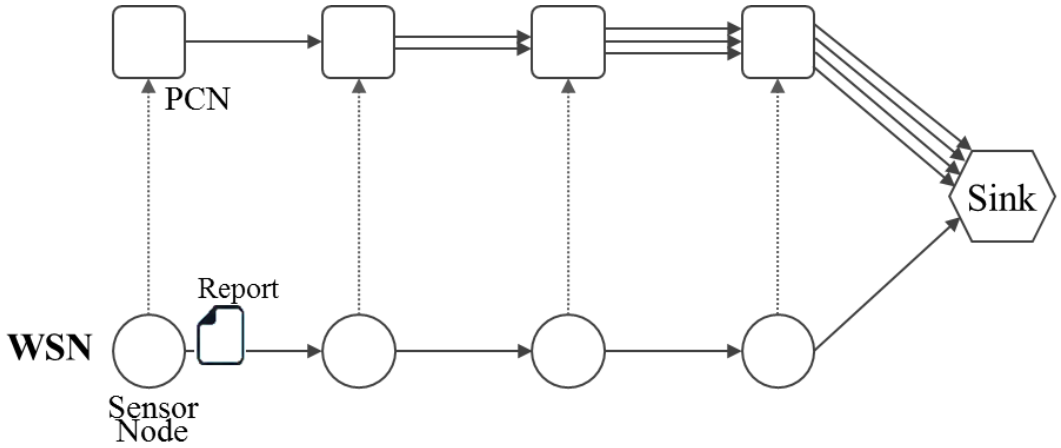

Figure 3:- Overview of the system described in [7]

As shown in Figure 3, the sensor network consists of a large of sensor nods, the sink, and PCNs in a sensor field. When a sensor node forwards a report after sensing an event, a PCN collects the report and forwards it to the sink. While the intermediate nodes broadcast it, the other PCNs also collect it and forward it. When the sink collects all of packets from the sensor field, the simulation models of the sink analyze the collected report and detects the compromised nodefor injecting false packets.

Motivation:-

In the WSN, sensor nodes are easily compromised by adversaries because they are deployed in an open collaborative environment. The compromised node can inject false reports into the sensor network. The false report causes energy to drain in intermediate nodes and causes a false alarm in the sink node. To deal with this attack, the SEF detects false MACs in the report in the intermediate nodes. It is difficult to detect the compromised nodes because they can modify sensitive data in packets even though the SEF effectively detects false reports. The scheme proposed in [7] detects the compromised nodes by analyzing data in a context aware architecture. We propose a simulation model for SEF that is designed and implementedbased on the scheme to effectively detect the compromised nodes against false report injection attacks. For inputs of the simulation, the collects all of packets such as [7]; for simulation outputs, it analyzes them to detect the compromised nodes.

Detection of Compromised Nodes using Modeling and Simulation:-

Assumption:-

We consider a sensor network that is composed of a sink node and a large number of sensor nodes (e.g. the Berkeley MICA2 motes[8]).The sink node is dependable due to a powerful sensor. The sensor nodes establish their routing path using Dijkstra's shortest path algorithm [9]. We further consider PCNs [7] to collect all of packets in the sensor field.

Overview:-

The sensor network is vulnerable to the false report injection attack injected in the compromised nodes because the network is operated in an open collaborative environment.To find the compromised nodes, the scheme proposed in [7] accurately detects them by analyzing data in a context aware architecture.

In this paper, we show the structure for detecting compromised nodes in a SEF-based WSN by applying the architecture proposed in [7].When the simulation model receives temporal data as described in [7], the data are stored according to the time sequence with time tag. This modelhas two subcomponent models (ANODE and CNTR) for analyzing the data in order to detect the compromised nodes. ANODE model compares the input data and outputs a data status to CNTR model; CNTE model analyzes the data status to detect compromised nodes. Thus, SEF-based simulation model effectively detects the compromised nodes.

Procedure in simulation models:-

The model detects compromisednodes exploiting the acquired temporal data as shown below.The collected data is transmitted to a node model (ANODE) corresponding to the sensor node when the sink receives the data via the PCNs. ANODE analyzes the collected date and transmits the analysis result to the controller model (CNTR). The CNTR detects the compromised node through comprehensive analysis.

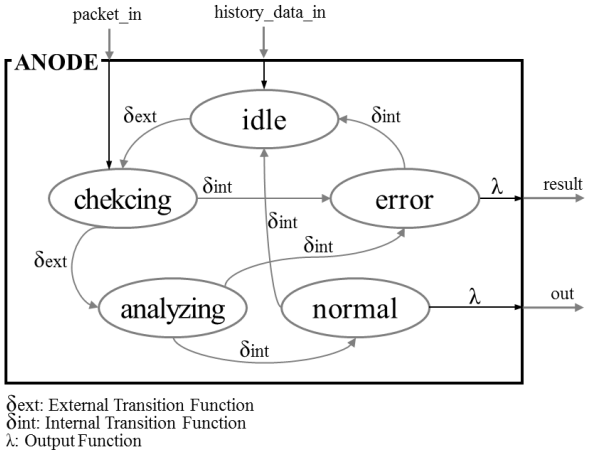

Figure 4:-ANODE model

Figure 4 shows an ANODE simulation model corresponding to the sensor node of the network. This model analyzes the collected data when the model receives the data through a port *packet_in* and infers the result. When this model receives a legitimate report, this node model's state transfers: *checking→analyzing→normal*. On the other hand, if the false report arrives at the model, its state transfers: *checking→analyzing→error*. The inference results are transmitted to the CNTR.

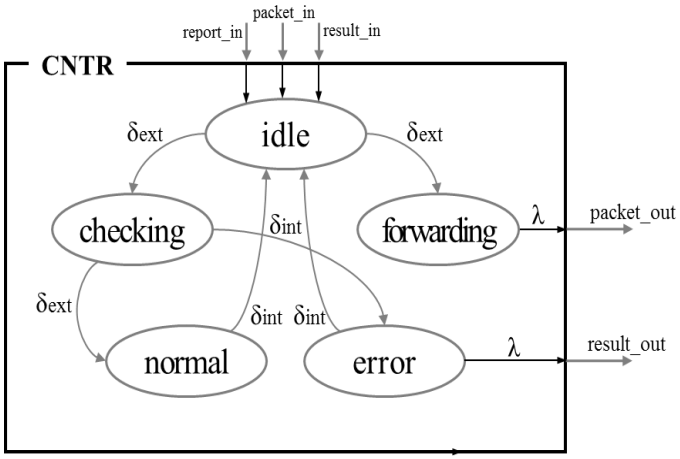

Figure 5:-CNTR model

Figure 5 shows the CNTR simulation model. This model selects the compromised node through a comprehensive analysis using the result. The CNTR provides information on the compromised node to the sink node.

Experimental Results:-

We performed an experiment to evaluate the proposed method compared to SEF. The sensor field contains 1000 sensor nodes in the WSN and 100 PCNs. Routing paths in the network were established based on Dijkstra's shortest path algorithm. Each node forwards reports toward the sink node via multiple hops. The sink node was located in the lower middle of the sensor field. Each node used 16.25 µJ per byte to transmit, 12.5 µJ per byte to receive, 15 µJ per byte to generate, and 75 µJ to verify a MAC in intermediate nodes [5]. The size of each report was 36 bytes. We randomly generated 300 events and set 10 compromised nodes for injecting false data in the sensor field. In addition, false reports were generated in the compromised nodes by a 10% probability. There was no packet loss in the experiment.

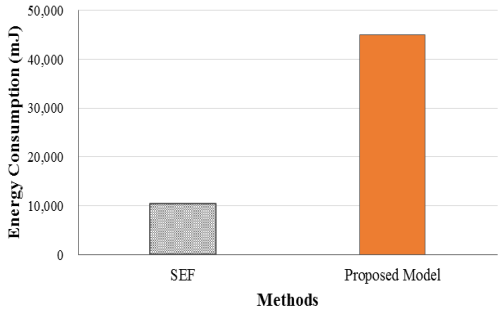

Figure 6:-Energy consumption in two methods

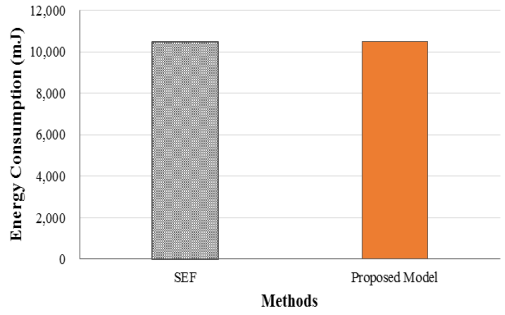

Figure 7:-Energy consumption in the sensor network

Figure 6 shows the energy consumption of SEF and the proposed method. As shown in Figure 7, the proposed model's energy consumption is higher than SEF because the PCNs in the proposed method forwards all collected data of the sensor network. However, as shown in Figure 9, the energy consumption of the two methods is the same. On the other hand, the proposed method does not request the energy resource of the sensor network.

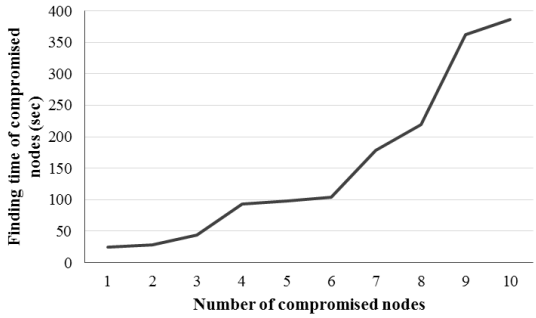

Figure 8:-Detection time of the compromised nodes in the sensor network

Figure 10 shows the detection time for finding compromised nodes in the sensor network. When the compromised nodes inject false data into the network, they are detected through the simulation methodology. All of them are detected within about 380 s. Thus, the proposed method detects all of the compromised nodes through the simulation methodology without any additional energy consumption of the sensor network.

Conclusion and Future Work:-

The sensor network is vulnerable to diverse attacks such as false report injection attacks since the sensors use wireless communication and have limited hardware resources. Even if the SEF protocol effectively detects false reports attack through the verification of multi-MACs against the false report injection attacks. The protocol is not capable of detecting compromised nodes when the attack occurs. The proposed modelsshowed the detection of the compromised nodes based on the temporal data acquired which in turn requires the system that exploits the data should be effectively store and process the data. This overall temporal processing is the main reason of the usage of the simulation models for the detection.

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. **I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam and E. Cayirci (2002)**, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114.

2. **K. Akkaya and M. Younis (2005)**, "A survey on routing protocols for wireless sensor networks," Ad Hoc Networks, vol. 3, pp. 325-349.

3. **X. Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks (2012)**," Sensors, vol. 12, pp. 11113-11153.

4. **S. M. Nam and T. H. Cho (2015)**, "A fuzzy rule-based path configuration method for LEAP in sensor networks," Ad Hoc Networks, vol. 31, pp. 63-79.

5. **F. Ye, H. Luo, S. Lu and L. Zhang (2005)**, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal On, vol. 23, pp. 839-850.

6. **F. Li, A. Srinivasan and J. Wu (2008)**, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Net-works," International Journal of Security and Network, vol. 3, pp. 173-182.

7. **S. M. Nam and T. H. Cho (2016)**, "Context-Aware Architecture for Probabilistic Voting-based Filtering Scheme in Sensor Networks," submitted to IEEE Transactions *on Mobile Computing*, TMC-2016-05-0332.

8. **Crossbow technology Inc**. http://www.xbow.com

9. **Fan Y., Chen A., Songwu L., and Lixia Z**. **(2001)**, "A scalable solution to minimum cost forwarding in large sensor networks," Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on. IEEE, pp. 304-309.