The ISC Int'l Journal of Information Security

ISeCure

January 2016, Volume 8, Number 1 (pp. 61–71)

http://www.isecure-journal.org

Unauthenticated Event Detection in Wireless Sensor Networks Using Sensors Co-Coverage☆

Meisam Kamarei [1,*], Ahmad Patooghy [2], and Mahdi Fazeli [2]

[1] *University of Applied Science & Technology, Tehran, Iran*

[2] *Department of Computer Engineering, Iran University of Science & Technology Tehran, Iran*

ARTICLE INFO.

Article history:

Received: 1 September 2015

First Revised: 11 January 2016

Last Revised: 25 January 2016

Accepted: 28 January 2016

Published Online: 31 January 2016

Keywords:

Attack, Wireless Sensor Networks, the More the Safe, the Less the Unsafe Policy, Unauthenticated Events.

ABSTRACT

Wireless Sensor Networks (WSNs) offer inherent packet redundancy since each point within the network area is covered by more than one sensor node. This phenomenon, which is known as sensors co-coverage, is used in this paper to detect unauthenticated events. Unauthenticated event broadcasting in a WSN imposes network congestion, worsens the packet loss rate, and increases the network energy congestion. In the proposed method, the more the safe, the less the unsafe (MSLU) method, each secure occurred event must be confirmed by various sensor nodes; otherwise the event is dropped. Indeed, the proposed method tends to forward event occurrence reports that are detected by various sensor nodes. The proposed method is evaluated by means of simulation as well as analytical modeling. A wide range of simulations, which are carried out using NS-2, show that the proposed method detects more than 85% of unauthenticated events. This comes at the cost of the network end-to-end delay of 20% because the proposed method does not impose delay on incoming packets. In addition, the proposed method is evaluated by means of an analytical model based on queuing networks. The model accurately estimates the network performance utilizing the proposed unauthenticated event detection method.

1 Introduction

Wireless Sensor Networks (WSNs) have been applied on several aspects of human life such as environmental monitoring, real-time target tracking, health care, animals behavioral monitoring, etc [1–4]. WSNs consist several sensor nodes and one or several base stations. Sensor nodes are very limited in hardware resources such as energy supply, processing unit, memory, and wireless bandwidth [5]. Therefore, energy consumption plays very important role in WSNs. Sensor nodes are established at environment for event detection. Thus sensor nodes are activated when an event occurs. Activated sensor nodes also make an event occurrence report and transfer it to the base station as real-time manner [6]. To the network energy consumption reduction, sensor nodes are unable to make direct communication with the base station. Therefore, multi-hop communication is natural in WSNs. Event detection and relay event occurrence reports within a specific environment to the base station are the main duty of sensor nodes [7]. With increase in WSNs applications, security and reliability play important role on these networks [8].

☆The submitted manuscript is an extended version of the work previously proposed in [27].

* Corresponding author.

Email addresses: kamarei@uast.ac.ir (M. Kamarei), patooghy@iust.ac.ir (A. Patooghy), m_fazeli@iust.ac.ir (M. Fazeli)

ISSN: 2008-2045

Harsh environmental conditions and a large number of sensor nodes imply that WSNs are implemented without any infrastructure [9]. Although, sensor nodes are very limited in computing resources, so they cannot perform complex processing on incoming data. Of course, event occurrence reports are usually as little data packet which they show occurred event details such as event location, event type, etc [10, 11]. On the other hand, sensor nodes usually receive and relay an event occurrence report toward the base station. This phenomenon increases attacker nodes ability to transpire within the network and they make and broadcast lot unauthenticated events into the network [12, 13].

After an unauthenticated event injection within the network by attacker nodes, the network congestion increases [12, 13]. Increase in the network congestion leads to increase in number of packets lost and the sensor nodes energy consumption. The sensor nodes energy consumption is one of the most important parameters of Quality-of-Service (QoS) in WSNs. The sensor nodes lifetime is dependent on their energy consumption. Thus, increase in the sensor nodes energy consumption leads to the sensor nodes death. With increase in the number of sensor nodes death, all points of the network may not be covered by sensor nodes. In fact the network coverage and the network lifetime are dependent on the network energy consumption. However, unauthenticated event broadcasting increases the network congestion as well as the network energy consumption.

Sensor nodes cannot perform complex processing on the incoming packets to unauthenticated events detection and elimination, due to constraint in their computing resource. Of course, limitation in the sensor nodes hardware resources such as transceiver unit and memory lead to they cannot make and transfer big data packets [6]. Thus data packets must not be equipped with a large number of redundant bits to unauthenticated events detection. Indeed, unauthenticated events detection with redundant bits is not suitable for WSNs. In this regard, researchers can find attacker nodes and do not let them to broadcast unauthenticated packets within the network instead unauthenticated packets detection [14]. Because WSNs are event driven and very redundant [15], therefore the number of event occurrence reports behalf various source nodes can be an efficient parameter to unauthenticated events detection, i.e., an event occurrence report with various source nodes is reliable and an event occurrence report with one source node is unreliable, with high probability.

In this paper an efficient method to defense against unauthenticated events broadcasting attacks in a WSN is proposed. The proposed method tries to recognize compromised nodes instead of unauthenticated events detection. The proposed method monitors sensor nodes activity to find attacker nodes. The proposed method acts based on the More the Safe, the Less the Unsafe, MSLU, policy for unauthenticated events detection. This policy considers the network is k-coverage wherein each point within the network is covered by more than one sensor node. Based on MSLU policy, event occurrence reports with various source nodes are reliable and event occurrence reports with a sensor node in unreliable with high probably. The proposed method without need to packet processing performs recognition of unauthenticated events and it does not allow unauthenticated events injection within the network by compromised nodes.

The rest of the paper is organized as follows: Section 2 summarizes the background and related work. In Section 3 the proposed unauthenticated events detection method is explained. Our proposed analytical model has been offered in Section 4. Simulation results are presented and discussed in Section 5. Finally, in Section 6 obtained results and future work are explained.

2 Related Work

WSNs are established at environment without any infrastructure. This phenomenon implies that several security attacks such as collision attack [16], unintelligent replay attack [12], unauthenticated broadcast attack [12], full domination attack [12], exhaustion attack [12], intelligent jamming attack [12, 17] threaten these networks. Unauthenticated broadcast attack is one of the most common security attacks in WSNs. Increase in the network congestion is the main purpose of the unauthenticated broadcast attack. Increase in the network congestion leads to the network energy consumption as well as increasing the posibility ofpackets lost. Recently, researchers have proposed several methods to detect unauthenticated events.

Unauthenticated events broadcasting attack is such MAC security attack in WSNs. In this case, compromised nodes broadcast a large number of unauthenticated events within the network to increase in network congestion as well as the network energy consumption. Unauthenticated events may be created and propagated as hello message or spurious event occurrence report [10]. The base station can distinguish unauthenticated events, but sensor nodes are unable to distinguish between original and unauthenticated events. Because wanderer packets within WSN are very small data packets which contain small information such as node ID or event occurrence report. On the other hand, sensor nodes are very limited in computing resources, so they cannot perform complex processing on incoming packets to recognize unauthenticated events.

In [18] a hop-by-hop filtering method has been proposed. In this method each node decrypts and encrypts the received data by gathering information from its next and pervious hops. However, the false data may be detected after passing from several hops and this phenomenon increases the network energy consumption. In [19] every node is equipped with some symmetric keys. In this regard, when an event occurs several neighborhood nodes of occurred event collaborate with each other to make an encrypted event occurrence report. This scheme focuses to improve filtering efficiency with a complex coding method. Therefore, complex coding method requires the powerful computing resources in sensor nodes. In [11] a method based on multipath data transferring scheme to unauthenticated events detection and filtering has been proposed, EEMDTS. EEMDTS method uses redundancy in routing algorithms as multipath routing to prevent access of event information by a compromised node. A method based on filtering scheme has been proposed in [10]. This method filters unauthenticated events based on the geographical information and the neighbor nodes information. A method for defending against denial-of-sleep attack has been offered in [12]. This method classifies denial-of-sleep attack based on attackers knowledge of MAC layer. A Virtual Energy Based Encryption and Keying, VEBEK, has been offered in [20]. VEBEK uses the residual energy of sensor nodes to data encryption on forwarded packets. Indeed, VEBEK encrypts transferred packets to unauthenticated events detection by sensor nodes. In [16] a method for collision attack has been proposed. In collision attack, compromised node causes network congestion and does not allow packet transmission by its neighbors. In [21] a secure MAC protocol has been proposed which acts based on CTS/RTS mechanism. In [22] a method to attack detection has been proposed which uses neural network to attack detection. A Dynamic En-route Filtering, DEF, has been proposed in [23]. DEF uses redundancy along forwarded packets as authentication keys. Then, receiver node can detect and drop unauthenticated event by authentication keys. The more related methods are very dependent on transferred packets. Dependency on data packets to recognize unauthenticated events increases the sensor node energy consumption as well as using powerful computing and processing resources. To improve the network performance, attacker nodes detection based on nodes behavior within the network is more efficient than unauthenticated events detection.

3 Unauthenticated Event Detection Method

In this section, we first introduce the more the safe, the less the unsafe, MSLU, policy and then we discuss the sensor nodes model, and our method to detect unauthenticated events within the network, respectively.

3.1 The More Safe, The Less Unsafe Policy

Reliability and performance such as energy consumption, message delay and hardware resources usage are the most important parameters to develop a protocol for WSNs. WSNs application require different levels of reliability, for example health and military WSN applications require message authentication & integrity [24]. Thus this section proposes a policy to make reliable data transferring in various applications of WSNs. In more WSNs applications, these networks act as a real-time and event driven network. Hence, we have assume a network that includes more sensor nodes and a base station in the network architecture. Therefore, more sensor nodes are distributed at environment to detect occurred events and report them to the base station. Also, we have assumed that these networks are very redundant such that each point within the network is covered by several sensor nodes. After each event occurrence, several sensor nodes detect and report it to the base station. An event occurrence report is reached to the base station as multi-hop communications manner by passing several intermediate nodes. In fact traffic pattern in a WSN is as many to one, i.e., several sensor nodes detect and report an event to a base station. This phenomenon leads to after each event occurrence, several same event occurrence reports behalf various source nodes are transferred to the base station. In this regard, the reliable event occurrence report must be made and reported by various source nodes. Natural redundancy and the network k-coverage are available solutions to increase the network security and reliability. We have used this approach to propose the More the Safe, the Less the Unsafe, MSLU, policy. In MSLU policy, event occurrence reports with various source nodes are reliable with high probably. Of course, unauthenticated events are made and injected within the network by a source node with high probability. Indeed MSLU considers that WSN is very redundant and it is k-coverage [25]. Figure 1, shows the network traffic after an occurred event. Based on this figure, sensor nodes that are inside occurred event radius detect and report it to the base station. This figure shows an occurred event that is considered as a reliable event by MSLU policy. MSLU acts based on natural redundancy in WSNs. This strategy leads to MSLU without requiring to impose computing cost in network detects attacker nodes. Therefore, in MSLU policy, reliable routing protocols do not require redundant code to false data detection. Because, MSLU policy tries to detect attacker nodes and it prevents packet injection within the network from attacker nodes. Of course,

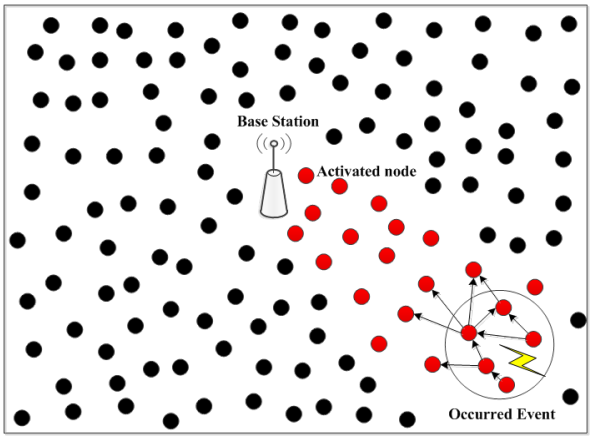

Figure 1. Traffic pattern in a WSN after an occurred event.

MSLU policy monitors sensor nodes behavior within the network and it controls transferring rate of sensor nodes to unauthenticated event detection.

3.2 Unauthenticated Events Detection

We use MSLU policy to propose an efficient method for an unauthenticated event detection and elimination. Our proposed method considers each sensor node has two input/output buffers to receive and forward the packets, according to Figure 2. The packets after arriving to a sensor node are placed into the input buffer. The incoming packets are serviced as first come-first served, FCFS, policy. Therefore, transferred packets are reached to output buffer and then they are sent to next hop. After forereach of packet service time in input buffer, the sensor node transfers it with $1-p$ probability. The sensor node does not transfer the packet and drops it with p probability . Of course, p parameter is a threshold value that it shows probability that incoming packet is an unauthenticated event or an authenticated packet. p parameter is calculated for each incoming packet based on MSLU policy. Thus p probability plays an important role in the proposed method for unauthenticated event detection.

After each event occurrence, several same packets are reached to input buffer of sensor nodes. These packets contain a little information about newly occurred event. Incoming packets show an occurred event report within the network. We assume that sensor nodes can distinguish among incoming packets, according to their source nodes. Each activated node imposes delay on the first incoming packet, until its input buffer be empty. When input buffer of activated node is empty then proposed method makes decision about the occurred event, i.e., the packet must be dropped or forwarded. In this regard, the occurred event transfers with $1-p$ probability and it drops with p probability. Therefore, proposed method makes decision about the first incoming packet, because several same packets

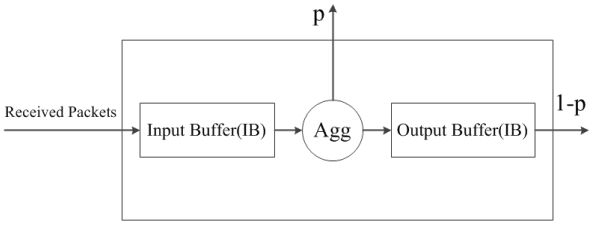

Figure 2. Structure of a typically sensor node [26].

of an occurred event are reached to a sensor node. Of course, the remaining incoming packets of input buffer are used to calculate p parameter. Proposed method tends to forward event occurrence reports that various sensor nodes are source of them.

The proposed method considers that the network is $k-$coverage, so after each event occurrence k packets of a newly occurred event are reached to a sensor node. The proposed method imposes delay to the first incoming packet as long as k packets service time. Departure packets change on p parameter based on their source node. When input buffer is empty, the proposed method makes decision about newly occurred event, i.e., the proposed method transfers or removes event occurrence report. p parameter is calculated by Equation (1).

$$p = e^{-\frac{R_e}{P_e}} \tag{1}$$

where, R_e is reward parameter of newly occurred event and P_e is penalty level of newly occurred event. After packets of a newly occurred event reach to input buffer of sensor nodes then these packets are serviced respectively. The proposed method penalizes repetitive packets and it rewards non repetitive packets. Indeed, if a received packet has been processed by the proposed method, then penalty parameter changes as Equation (3). This case shows that sensor node received a repetitive packet. Repetitive packets have same source node. On the other hand, if received packet had not seen yet, then proposed method rewards it as Equation (2).

$$R_e = R_e + 1 \tag{2}$$

$$P_e = P_e + 1 \tag{3}$$

Initially that a newly event occurs and input buffer of sensor nodes is empty, R_e and P_e are as Equation (4) and Equation (5).

$$R_e = 1 \tag{4}$$

$$P_e = 1 \tag{5}$$

The pseudo-code of the proposed method is shown in 1. According to this Algorithm, the proposed method makes decision about each event occurrence report based on MSLU policy, i.e., a newly occurred event must be reported to the base station or it must not inject within the network. Each event occurrence report that has been made by a source node, with high

probably is an unauthenticated event. Thus, the proposed method reduces its forwarding chance, i.e., the proposed method penalizes these event occurrence reports. On the other hand, event occurrence reports with various source nodes are rewarded by the proposed method. Indeed, the proposed method increases their forwarding chance.

The proposed method detects unauthenticated events based on the more the safe, the less the unsafe policy. Thus, the proposed method considers that packets of an occurred event on behalf of a source node are unauthenticated events with high probably . The proposed method transfers an event occurrence report toward the base station with $1-p$ probability and drops it with probability p. Indeed, the proposed method detects unauthenticated events with p probability. The proposed method considers WSN is $k-$coverage and the network acts as event driven and real time manner. In fact, the proposed method considers after each event occurrence, several data packets are made and transferred toward the base station. The proposed method tends to forward event occurrence reports with various source nodes and it does not tend to forward event occurrence reports with less source nodes. Indeed, the proposed method monitors nodes behavior to attacker nodes detection and does not allow packets injection within the network from attacker nodes.

Algorithm 1 Pseudo-code of the proposed method.

Input: k packets of a newly occurred event
Output: Event occurrence transferring or removing
$P_e \leftarrow 1$;
$R_e \leftarrow 1$;
When input buffer is not empty
Begin
if received packet is repetitive **then**
$P_e \leftarrow P_e + 1$
else
$R_e \leftarrow R_e + 1$
end if
End
$p \leftarrow e^{-\frac{R_e}{P_e}}$
$re \leftarrow$ a random number between 0 and 1
if $re \leq p$ **then**
Event occurrence report must be removed
else
Event occurrence report must be sent
end if

4 Analytical Modeling

Multi-hop communications from environment to the base station results in a layered WSN. In a layered WSN, sensor nodes are located on 0-th layer and the base station is located on l-th layer. Therefore, intermediate nodes are located from 1st layer to $l-1$-th layer. WSNs can be shown and evaluated as multilayer model. The proposed analytical model evaluates our proposed method based on an analytical multilayer model. In Section 3, we have offered a method for unauthenticated event detection in a redundant wireless sensor network. The proposed method considers each point within the network is covered by at least k sensor nodes. The probability of a network to be k-coverage is discussed in Equations (6) and (7).

$$z = \frac{\pi r_s^2}{N_s} \tag{6}$$

$$P[\text{network to be } k-\text{coverage}] = \begin{cases} \zeta & \text{if} \quad \zeta \leqslant 1 \\ 1 & \text{if} \quad \zeta > 1 \end{cases} \tag{7}$$

where $\zeta = \binom{n}{k} \times z^k \times (1-z^{n-k})$, N_s is the network space, r_s is sense radius of sensor nodes, and n is number of sensor nodes within the network. The proposed method can be modeled as a network of queues as shown in Figure 3. We have proposed this model in [4]. Based on multi-hop communication pattern in WSNs, the proposed model shows a WSN in l layers. Sensor nodes are in 0-th layer and the base station is located in l-th layer. Therefore, sensor nodes within 1st layer and $l-1$ -th layer are intermediate nodes from environment to the base station. By our proposed method, an unauthenticated event report is detected in 0-th layer with high probably. In fact, one hop neighborhood of an occurred event plays very important role to detect an unauthenticated event in the proposed method. Thus, the proposed method considers 0-th layer is unsafe. Indeed, after unauthenticated event reports filtering in 0-th layer, authenticated event reports are reached to the base station by intermediate nodes.

Input queue of sensor nodes capacity has large impact on the proposed method performance. The proposed analytical model evaluates input queues capacity versus the proposed method performance. The proposed method performance is considered as unauthenticated events detection. We evaluate this parameter in unsafe part of the network, i.e. 0-th layer denotes unsafe part. Packets arrival rate to input queue of the sensor node in 0-th layer, λ_{IB_0}, is calculated by Equation (8).

$$\lambda_{IB\_0} = k \times \lambda \tag{8}$$

where λ is event occurrence rate (event/time unit). Packet departure rate from input queue of sensor nodes within 0-th layer is calculated by Equation (9).

$$X_{T\_IB0} = \lambda_{IB\_0} \times (1 - P_{IB\_0}) \tag{9}$$

Input queue of sensor nodes have finite capacity that are modeled as an M/M/1/K queue. Thus P_{IB_0} is the probability of an input queue being filled that is calculated by Equations (10) and (11).

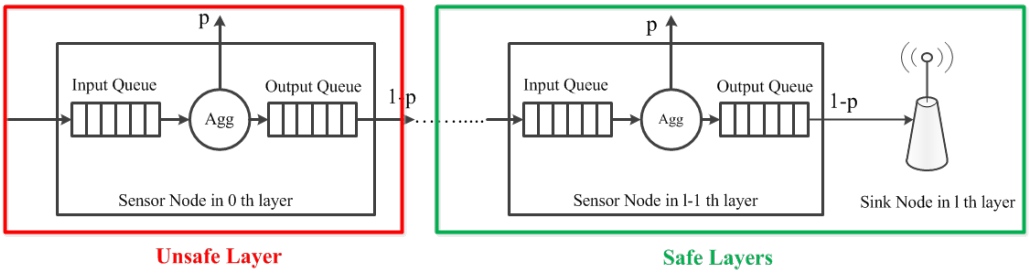

Figure 3. Proposed Model.

$$r = \frac{\lambda_{IB\_0}}{\mu} \tag{10}$$

$$P_{IB\_0} = \frac{(1-r) \times r^{B}}{1 - r^{B+1}} \tag{11}$$

where μ is mean packet service time and B is input queue capacity. Departure packets from input queues are transferred to the base station with p probability. Equation (12) calculates the sensor node transfer rate in 0-th layer, X_{S_0}.

$$X_{S\_0} = (1-p) \times X_{T\_IB0} \tag{12}$$

We evaluate input queue capacity, B, versus probability of unauthenticated events detection. Input queue capacity, B, has direct relationship with probability of unauthenticated event detection. However, an input queue with more capacity increases the network end to end delay. Equation (13) calculates the number of false packets that report an unauthenticated event within input queue of the sensor node in 0-th layer. Parameter z_c denotes percentage of compromised nodes within the network. Based on Equation (13), unauthenticated event rate is proportional with percentage of compromised nodes. In fact, compromised nodes inject more unauthenticated event reports within the network and increase input queue incoming ratio. Therefore, number of unauthenticated event reports into the input queues is one of the most important parameters to unauthenticated event detection by the proposed method.

$$P[\alpha = B] = \binom{B}{\alpha} \times z_c^{\alpha} \times (1 - z_c)^{B-\alpha} \tag{13}$$

where α is number of false packets within input queue. The proposed method detects an unauthenticated event based on number of its source nodes. Based on Equation (1), incoming packets with same source node increase probability of unauthenticated event detection. $\alpha > \frac{B}{2}$ decreases the probability of event occurrence forwarding by sensor node in 0-th layer. Therefore, the proposed method tends to forward event occurrence reports with $\alpha < \frac{B}{2}$. Also, when $\alpha = \frac{B}{2}$ the proposed method sends or does not send event occurrence report with same probability. Figure 4, shows probability of unauthenticated event detection, p, versus parameter B based on Equation (13). We consider $\alpha = \lfloor \frac{B}{2} \rfloor$ and parameter z_c is 10%, 20%, 30%, 40%, 50% and 60% respectively. In Figure 4, probability of unauthenticated event detection, p, has been calculated by Equations (14) and (15). Equation (14) comes from Equation (1), i.e. v_e is reward parameter and α is penalty parameter. In Equation (15), parameter k denotes the network $k-$coverage and X_{T_IB0} is packet departure rate from input queue of sensor nodes (See Equation 9). Our proposed method is dependent on incoming packets into input queue of sensor nodes. Therefore, number of compromised nodes has direct relationship with number of false packets incoming rate within input queue. When number of false packets and reliable packets within input queue are balanced, our proposed method has inefficient performance to unauthenticated event detection (See Figure 4.b to Figure 4.e). On the other hand, more reliable packets or more false packets within input queue increases or decreases event occurrence report forwarding chance respectively (See Figure 4.a and Figure 4.f). Therefore, we consider $\alpha = \lfloor \frac{B}{2} \rfloor$ in Figure 4. Thus in Figure 4, two even & odd continuous points has same value in α parameter, i.e., α in 8 and 9 points is equal to 4. However in 9 point number of reliable packets in incoming queue are 5 packets and false packets are 4 packets as result probability of unauthenticated event detection in 9 point is greater than 8 point. This phenomenon leads to the zigzag behavior of the curves in Figure 4.

$$p = \begin{cases} \eta & \text{if} \quad \eta \leqslant 1 \\ 1 & \text{if} \quad \eta > 1 \end{cases} \tag{14}$$

where $\eta = X_{T\_IB0} \times P[\alpha = B] \times e^{-\frac{v_e}{\alpha}}$ and

$$v_e = \begin{cases} B - \alpha & \text{if} \quad B \leqslant 2k \\ k & \text{if} \quad B \geqslant 2k \end{cases} \tag{15}$$

According to Figure 4, it can be seen that increase in input buffer size, B, leads to an increase in probability of unauthenticated event detection, p. In fact the input buffer size, B, has direct relationship with probability of unauthenticated event detection, p With increase in the input buffer size, B, more false packets of an unauthenticated event can be reached to input buffer' sensor nodes. Therefore, $\alpha > \frac{B}{2}$ increases parameter p. On the other hand, $B = 2k$ is a threshold value that

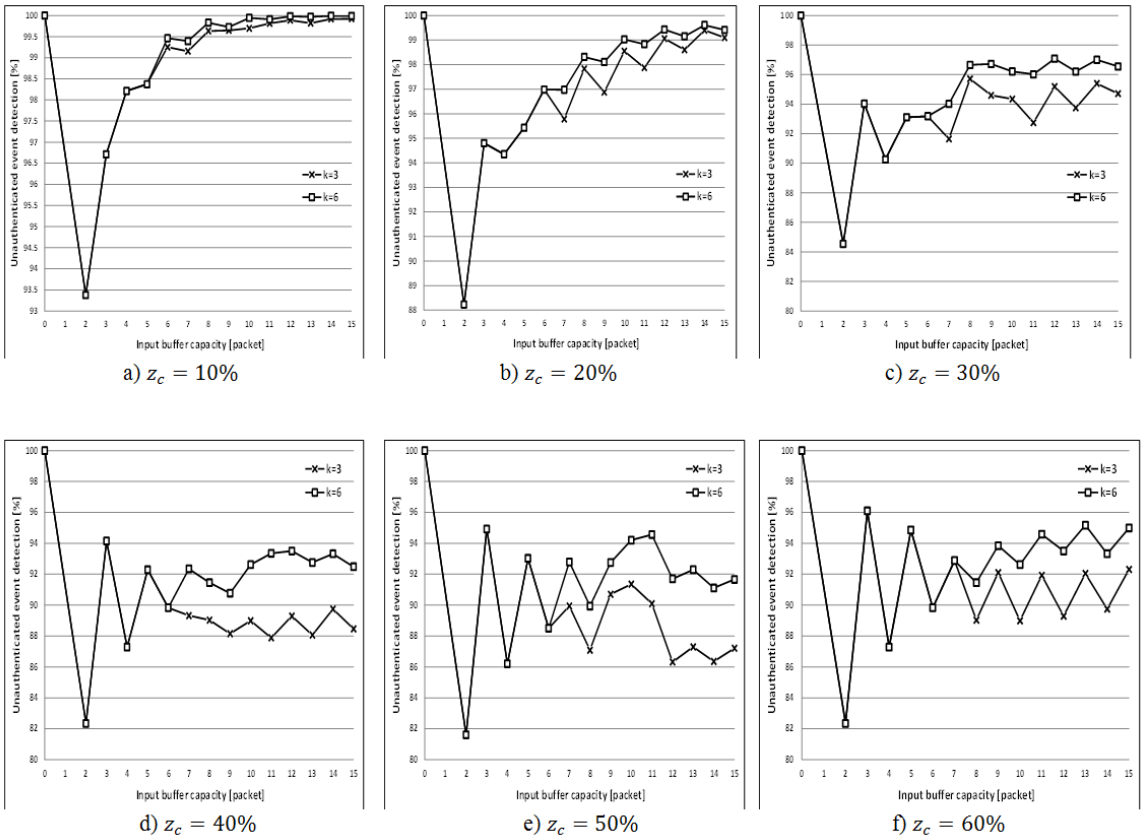

Figure 4. Input buffer capacity vs. Unauthenticated event detection.

parameter p is increasing here. However, sensor nodes are very limited on their hardware resources. Thus, based on our proposed analytical model, $B = 2k$ is an acceptable value for input buffer size, B.

5 Experimental Results

In this section, the proposed method performance is evaluated via NS-2.35 simulator. Different parameters of simulation are presented in Table 1. Communication parameters for WSN are adopted based . Also, the general parameters required for energy consumption are adopted from . In Table 1, e_{rx} is the energy consumed by electronic circuit for receiving or forwarding one bit of data, e_{tx} is the energy consumed by sender node for forwarding one packet and e_a is energy consumption for alive state of sensor nodes. e_{att} is energy consumption of sensor nodes for unauthenticated event detection. Because, the proposed method does not process packets to unauthenticated event detection, e_{att} in the proposed method is equal to e_{rx}. WSNs are event driven network which after each event occurrence the network traffic increases. Thus, the network traffic is dependent on event occurrence rate. In Table 1, λ is event occurrence rate (event/time unit). *Filtering efficiency* is defined as the percentage of unauthenticated events which to be filtered within a specified number

Table 1. Simulation Parameters.

Terrain	$1000m \times 1000m$
Node Number	500
Radio Range	250 m
Sim Time	100 S
Initial Node Energy	1000 J
Propagation Model	Two Ray
Number of compromised nodes	20-30%
λ	2 event/s
e_{rx}	$0.1\mu J$
e_{tx}	$0.33\mu J$
e_a	$0.05\mu J$
e_{att}	$0.1\mu J$

of nodes effectively . The proposed method detects unauthenticated events based on MSLU policy. In the proposed method, if a compromised node broadcasts a lot of unauthenticated events, first its one-hop neighborhood detects it. Therefore, one-hop neighborhood does not allow to be propagated more unauthenticated events. Figure 5, shows filtring efficiency of the

proposed method with previous methods EMDTS , DEF , VEBEK . According to Figure 5, it can be seen that the proposed method filtrs 88% unauthenticated events within 2 nodes. EEMDTS filters 60% of unauthenticated events within 2 nodes, VEBEK filters 50% of unauthenticated events within 2 nodes and DEF filters 47% of unauthenticated events within 2 nodes. However, EEMDTS filters 95% of unauthenticated events within 5 nodes, VEBEK filters 90% of unauthenticated events within 10 nodes and DEF filters 90% of unauthenticated events within 12 nodes. Figure 6, shows the average number of nodes that unauthenticated events are transferred versus number of compromised nodes. Because, in the proposed method one hop neighbor of compromised node plays important role to unauthenticated event detection, so increase in number of compromised nodes in the network no effect on number of receiver nodes of unauthenticated event. Therefore, in proposed method the number of traveled nodes by unauthenticated event is identical versus number of compromised nodes.

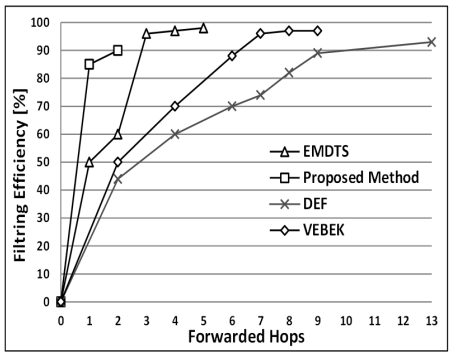

Figure 5. Unauthenticated event filtering efficiency.

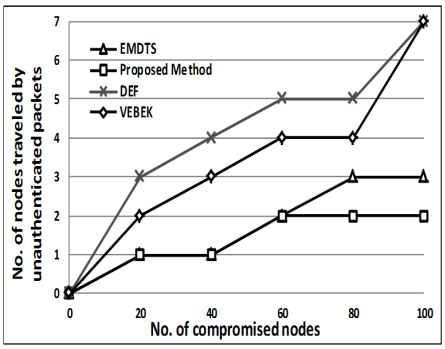

Figure 6. Number of hops traveled by unauthenticated event vs. compromised node.

Our proposed method is compared with a deterministic approach. In a deterministic approach, an occurred event is considered as an unauthenticated event if there are i false packets of newly occurred event within input queue of sensor nodes. Figure 7, shows packets distribution into input queue of sensor nodes after each event occurrence. In this figure, input queue of sensor nodes capacity, B, is five packets. After each event occurrence, several sensor nodes that have detected the occurred event transfer event occurrence report to the base station immediately. Therefore, compromised nodes always inject more false packets within the network. Thus reliable event occurrence reports and false packets are reached to input queue of sensor nodes to gather. False and reliable packets are reached to input queue of sensor nodes randomly. Number of false and reliable incoming packets within an input queue of sensor node are different according to Figure 7. On the other hand, if input queue is to be filled, false or reliable packets cannot reach to input queue and they are eliminated. In a deterministic approach, we consider an occurred event is unauthenticated event if number of false packets within input queues is greater than 1, 2, 3, 4 and 5 packets. Table 2, shows deterministic and probabilistic comparison to reliable event forwarding by a sensor node. The probabilistic approach uses the proposed method to send/remove an occurred event report. Our proposed method is compared with a deterministic approach in remain scenarios . In these scenarios dp is deterministic parameter to filter unauthenticated events. Therefore, input queue capacity, B, is 10 packets in remain scenarios. Figure 8, shows amount of the network energy consumption to unauthenticated events detection with a deterministic approach and our proposed method. The proposed method filters unauthenticated events efficiently. Of course, the proposed method filters more number of unauthenticated events by one-hop neighbor of compromised nodes. In this case, the network congestion does not increase by unauthenticated events. Therefore, the proposed method aggregates redundant packets of an occurred event. Thus, the proposed method reduces the network traffic as well as the network energy consumption. On the other hand, in deterministic approach sensor nodes remove more incoming packets with increase in number of compromised nodes. Large number of packets removing from input queue decreases the network energy consumption in deterministic approach. Figure 9, shows packets delivery ratio to the base station versus the number of compromised nodes. Compromised nodes increase the network congestion by increase in the number of unauthenticated events injection within the network. Of course, in the proposed method, input queue of sensor nodes has limited capacity. Thus, it is possible that several data packets cannot reach to input queue of sensor node and they are eliminated when input queue is filled. In our proposed method, packet delivery ratio to the base station decreases, when the network congestion increases. Therefore, large number packets removing from input queue leads to decrease packet delivery ratio by a deterministic approach. On the other hand,

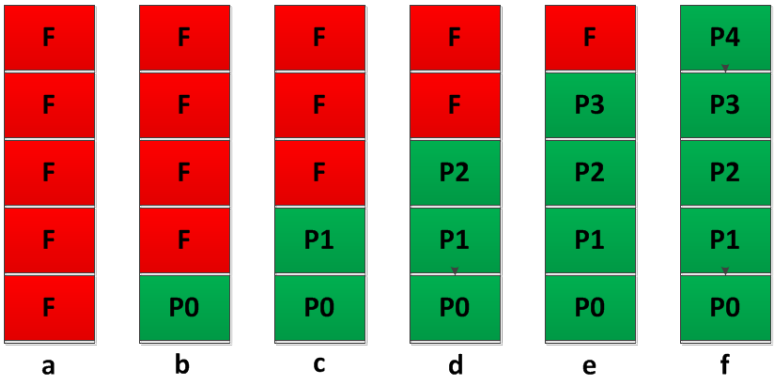

Figure 7. Packets distribution in input queue of sensor nodes after an event occurrence.

Table 2. Deterministic and Probabilistic Approach Comparison.

	Deterministic Approach					Probabilistic Approach					
	Deterministic Parameter (DP)										
	1	2	3	4	5	Figure 7.a	Figure 7.b	Figure 7.c	Figure 7.d	Figure 7.e	Figure 7.f
Authenticated Event Forwarding [%]	16.5	33	49.5	66	83	15	32	52	73	91	99

the proposed method can recognize and eliminate more unauthenticated events within the network. Figure 10, shows number of compromised nodes versus filtering efficiency. In our proposed method, increase in number of compromised nodes leads to increase in event occurrence report elimination, i.e., parameter p increases here. Besides, in a deterministic approach with decrease in parameter dp a reliable event must be authenticated by more sensor nodes. Although, when $dp = 3$ a reliable event is forwarded if more than seven authenticated packets are reached to input queue. This phenomenon decreases reliable event occurrence forwarding chance as well as filtering efficiency. Figure 1, shows the number of compromised nodes versus the network end to end delay. Based on this figure, it can be seen that increase in number of compromised nodes leads to increase in the network end to end delay. More compromised nodes within the network increase the network traffic as well as the network congestion. Thus, the network congestion leads to increase in the network end to end delay. However, excessive packets removing decreases the network congestion as well as the network end-to-end delay in the deterministic approach.

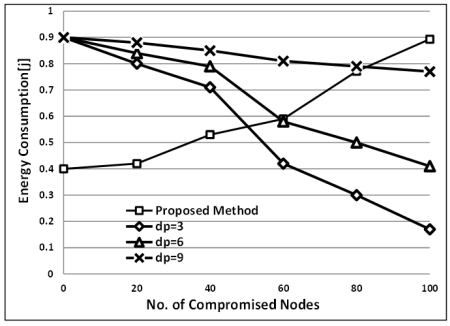

Figure 8. The network energy consumption vs. number of compromised nodes.

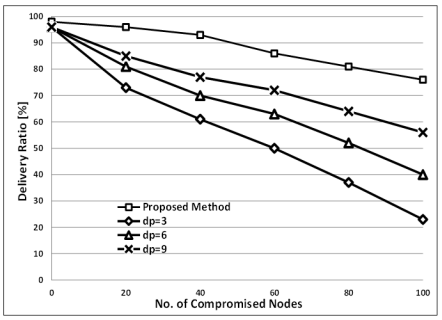

Figure 9. Packet delivery ratio vs. number of compromised nodes.

6 Conclusion

Wireless sensor networks are threatened by various security attacks. Because, these networks are established at harsh environment and the network operates without any surveillance. In this case, unauthenticated events propagation within the network to increase in the network energy consumption is a popular attack in wireless sensor networks. In this paper, an efficient method based on the more the safe, the less the unsafe policy to unauthenticated events recognition and dropping was proposed. The more the safe, the less the unsafe policy considers the network is redundant and k-coverage. Thus each reliable event must be de-

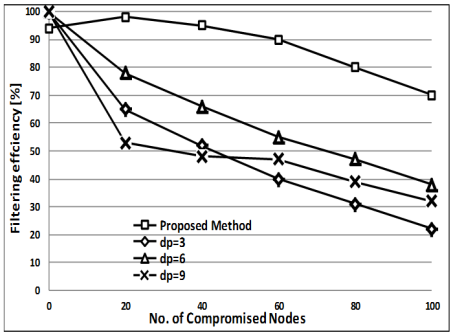

Figure 10. Filtering efficiency vs. compromised nodes.

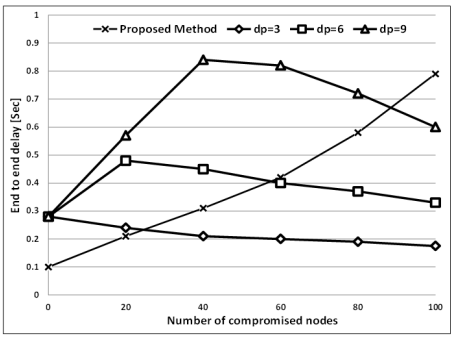

Figure 11. The network end-to-end delay vs. compromised nodes.

tected and reported by several sensor nodes. Therefore, lot transferring packets from a source node are unauthenticated events with high probably. The proposed method tends to inject event occurrence reports within the network that they are reported by various source nodes. Of course, the proposed method tries to recognize comprised nodes and filter their transferring packets instead false data detection.

References

[1] J. Feng, Z. Wang, and J. Henkel, "An Adaptive Data Gathering Strategy for Target Tracking in Cluster-based Wireless Sensor Networks," in IEEE Symposium on Computers and Communications (ISCC), Cappadocia, 2012, pp. 468-474.

[2] S. Bhattacharjee, P. Roy, S. Ghosh, S. Misra, and M. S. Obaidat, "Wireless sensor network-based fire detection, alarming, monitoring and prevention system for Bord-and-Pillar coal mines," The Journal of Systems and Software, vol. 85, pp. 571-581, 2012.

[3] M. J. Chae, H. S. Yoo, J. Y. Kim, and M. Y. Cho, "Development of a wireless sensor network system for suspension bridge health monitoring," Automation in Construction, vol. 21, p. 237252, 2012.

[4] M. Kamarei, M. Hajimohammadi, A. Patooghy, and M. Fazeli, "An Efficient Data Aggregation Method for Event-Driven WSNs: A Modeling & Evaluation Approach," Wireless Personal Communications an International Journal, vol. 84, no. 1, pp. 745-764, 2015.

[5] J. H. Ho, H. C. Shih, Y. B. Liao, and S. C. Chu, "A ladder diffusion algorithm using ant colony optimization for wireless sensor networks," Information Sciences, vol. 192, no. 1, p. 204212, 2011.

[6] M. E. Keskin, I. K. Altnel, N. Aras, and C. Ersoy, "Wireless sensor network lifetime maximization by optimal sensor deployment, activity scheduling, data routing and sink mobility," Ad Hoc Networks, vol. 17, p. 1836, 2014.

[7] S. Cheng and T. Y. Chang, "An adaptive learning scheme for load balancing with zone partition in multi-sink wireless sensor network," Expert Systems with Applications, vol. 39, p. 94279434, 2012.

[8] P. Thao and C. H. Tae, "A multi-path interleaved hop-by-hop en-route filtering scheme in wireless sensor networks," Computer Communications, vol. 33, p. 12021209, 2010.

[9] R. S. Sachan, M. Wazid, A. Katal, D. P. Singh, and R. H. Goudar, "A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN," in International conference on Communication and Signal Processing, India, 2013, pp. 795-801.

[10] J. Wang, Z. Liu, S. Zhang, and X. Zhang, "Defending collaborative false data injection attacks in wireless sensor networks," Information Sciences, vol. 254, p. 3953, 2014.

[11] S. V. Annlin Jeba and B. Paramasivan, "Energy efficient multipath data transfer scheme to mitigate false data injection attack in wireless sensor networks," Computers and Electrical Engineering, vol. 39, p. 18671879, 2013.

[12] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 367-380, 2009.

[13] P. M. Pawar, R. H. Nielsen, N. R. Prasad, S. Ohmori, and R. Prasad, "Behavioral Modeling of WSN MAC Layer Security Attacks: A Sequential UML Approach," Journal of Cyber Security and Mobility, vol. 1, no. 1, pp. 65-82, 2012.

[14] M. Kamarei, A. Patooghy, M. Fazeli, and M. J. Salehi, "AT2A: Defending Unauthenticated Broadcast Attacks in Mobile Wireless Sensor Networks," International Journal of Electronics Communication and Computer Engineering, vol. 5, no. 5, pp. 1216-1221, 2014.

[15] A. Patooghy, M. Kamarei, A. Farajzadeh, F. Tavakoli, and M. Saeidmanesh, "Load-Balancing Enhancement by a Mobile Data Collector in Wireless Sensor Networks," in Eighth International

Conference on Sensing Technology, Liverpool, UK, 2014, pp. 634-638.
[16] P. Reindl, K. Nygard, and X. Du, "Defending malicious collision attacks in wireless sensor networks," in 8th International Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, 2010, pp. 771-776.
[17] W. Yee, et al., "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," ACM Transactions on Sensor Networks (TOSN), vol. 5, no. 1, pp. 1-6, 2009.
[18] S. Zhu, S. Setia, and S. Jajodia, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in Proceeding IEEE symposium on Security and privacy, 2004, p. 259271.
[19] F. Ye, H. Luo, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in Proceedings of 23th Annual Joint Conferenceof the IEEE Computer and Communications Societies, 2004, p. 24462457.
[20] A. S. Uluagac, R. A. Beyah, L. Yingshu , and J. A. Copeland, "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 994-1007, 2010.
[21] Q. Ren and Q. Liang, "Secure media access control (MAC) in wireless sensor networks: intrusion detections and countermeasures," in 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2004, pp. 3025-3029.
[22] M. V. Ramesh, A. B. Raj, and T. Hemalatha, "Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks," in Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, 2012, pp. 783-787.
[23] Y. Zhen and G. Yong, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," IEEE Trans Network, vol. 18, no. 1, pp. 150-163, 2010.
[24] N. Bandirmali and I. Erturk, "WSNSec: A scalable data link layer security protocol for WSNs," Ad Hoc Networks, vol. 10, pp. 37-45, 2012.
[25] J. Zhu and S. Papavassiliou, "On the Connectivity Modeling and the Tradeoffs between Reliability and Energy Efficiency in Large Scale Wireless Sensor Networks," in IEEE Wireless Communications and Networking, WCNC, New Orleans, LA, USA, 2003, pp. 1260-1265.
[26] M. Kamarei, M. Hajimohammadi, A. Patooghy, and M. Fazeli, "OLDA: An Efficient On-Line Data Aggregation Method for Wireless Sensor Networks," in Eighth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2013), Compiegne, France, 2013, pp. 49-53.
[27] M. Kamarei, A. H. Nasrollah Barati, A. Patooghy, and M. Fazeli, "The More the Safe, the Less the Unsafe: An efficient method to unauthenticated packets detection in WSNs," in 7th Conference on Information and Knowledge Technology (IKT), Urmia, Iran, 2015, pp. 1-6.

Meisam Kamarei received his M.S. in computer engineering from Islamic Azad University, Arak Branch, Arak, Iran, in 2013. He is currently a faculty member at University of Applied Science & Technology (UAST), Tehran, Iran. His current research interests include data aggregation, routing algorithms, modeling and evaluation, and security in wireless sensor networks.

Ahmad Patooghy received his M.S. and Ph.D. in computer engineering from Sharif University of Technology, Tehran, Iran, in 2005 and 2011, respectively. He is currently an assistance processor at department of computer engineering, Iran University of Science and Technology, Tehran, Iran. His research interests include hardware design and test, architectural design of multi-core and many-core chips, dependability and security evaluation of VLSI circuits, fault injection, and analytical modeling.

Mahdi Fazeli received the M.S. and Ph.D. degree in computer engineering from the Sharif University of Technology, Tehran, Iran, in 2005 and 2011, respectively. He has been with the department of computer engineering, Iran University of Science and Technology (IUST), since 2011, where he is currently an assistant professor. He has established and chaired the Networked and Embedded System Laboratory (NESL) at IUST, since 2012. He has authored or co-authored more than 40 papers in reputable journals and conferences. His current research interests include reliable issues in VLSI circuits and emerging technologies, hardware security, dependable embedded systems, Low power circuits and systems, fault-tolerant computer architectures, and reliability modeling and evaluation.

The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (p. 89)
http://www.isecure-journal.org

Persian Abstract

کشف رویدادهای احراز هویت نشده در شبکه‌های حسگر بی‌سیم با استفاده از ویژگی چند پوششی گره‌های حسگر

میثم کمره‌ئی[1]، احمد پاطوقی[2] و مهدی فاضلی[2]

[1]دانشگاه جامع علمی و کاربردی، تهران، ایران
[2]دانشگاه علم و صنعت ایران، تهران، ایران

افزونگی در شبکه‌های حسگر بی سیم مساله‌ای بدیهی است به شکلی که هر نقطه درون محدوده شبکه توسط چند گره پوشش داده می‌شود. در این مقاله از این پدیده که به صورت چند پوششی گره‌های حسگر شناخته می‌شود جهت شناسایی رویدادهای احراز هویت نشده استفاده می‌شود. انتشار رویدادهای احراز هویت نشده در یک شبکه حسگر بی‌سیم باعث ازدحام شبکه، افزایش احتمال از بین رفتن بسته‌ها و افزایش مصرف انرژی شبکه می‌گردد. در روش پیشنهادی که مبتنی بر رویکرد هر چه بیشتر امن‌تر و هر چه کمتر نا امن‌تر است، هر رویداد امن باید توسط چند گره مختلف تایید گردد؛ در غیر اینصورت رویداد از شبکه حذف می‌گردد. در واقع روش پیشنهادی تمایل به ارسال رویدادهایی دارد که توسط چندین گره حسگر کشف شده اند. روش پیشنهادی به وسیله شبیه‌سازی و مدل‌سازی تحلیلی مورد ارزیابی واقع شده است. نتایج شبیه سازی‌ها که وسیله شبیه ساز ns-2 پیاده سازی شده‌اند نشان می‌دهد که روش پیشنهادی بیش از ۸۵ در صد رویدادهای جعلی را کشف می‌کند. همچنین به دلیل عدم تحمیل تأخیر به بسته‌های ورودی، روش پیشنهادی ۲۰ در صد تأخیر انتها به انتهای شبکه را نیز کاهش می‌دهد. همچنین روش پیشنهادی توسط یک مدل تحلیلی مبتنی بر شبکه‌های صف مورد ارزیابی قرار گرفته است. مدل پیشنهادی با دقت بالایی کارایی روش پیشنهادی را جهت کشف رویدادهای جعلی تخمین می‌زند.

واژه‌های کلیدی: حمله، شبکه‌های حسگر بی‌سیم، مکانیزم هر چه بیشتر امن‌تر هر چه کمتر نا امن‌تر، رویدادهای احراز هویت نشده.