Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 06, No. 01, March 2020.

# THE IMPACT OF MOBILITY MODELS ON THE PERFORMANCE OF AUTHENTICATION SERVICES IN WIRELESS SENSOR NETWORKS

Iman Almomani[1] and Katrina Sundus[2]

*(Received: 20-Jul.-2019, Revised: 3-Nov.-2019, Accepted: 30-Nov.-2019)*


## *ABSTRACT*

*The applications of Wireless Sensor Networks (WSNs) are very important nowadays and could be found in many different life aspects. Broadcast authentication (BA) protocols are solutions to guarantee that commands and requests sent by the Base Station (BS), which controls the services provided by WSN, are authentic. Network mobility is considered one of the main challenges that WSN services in general and authentication protocols in particular are facing. Existing BA protocols did not give much attention to the effect of mobile BS or/and sensors on the behaviour of their protocols. Consequently, this paper provides a deep analysis of the impact of mobility on the performance of BA protocols. Three standard designs for BA protocols were studied in this research; Forwarding First (FF), Authentication First (AF) and Adaptive Window (AW). These three standard protocols were examined against four major mobility models. The results revealed that BA protocols behaved differently in terms of energy consumption and network delay with respect to mobility. For example, the delay in AW protocol was decreased by 47.6% in case of having fully mobile WSN; whereas the wasted energy was reduced by 37.5% in case of static BS and mobile sensors. Although the same authentication technique was applied in all three protocols, the mobility itself was a reason to enhance or degrade the performance of the authentication service which consequently affects the security of WSNs and their provided services. For example, when the BS was mobile and the sensor nodes were static, FF protocol decreased the delay by up to 98.81% compared to AF protocol and by up to 93.62% compared to AW protocol. On the other hand, AW Protocol saved the network energy by up to 94.49% compared to FF protocol and by up to 65.5% compared to AF protocol.*



## *KEYWORDS*

*Authentication, Wireless sensor network (WSN), Security, Mobility, Broadcast authentication, Adaptive window protocol, Authentication first protocol, Forwarding first protocol, Internet of Things (IoT), Digital signature.*


## 1. INTRODUCTION

Wireless sensor Network (WSN) is a group of spatially deployed sensor nodes that acknowledge or remotely observe diverse environmental variables or natural events [1]. WSN is currently practiced at various applications in both civilian and military fields [2]-[3]. Internet of Things (IoT) has become part of our daily life routines and its applications can be seen almost everywhere, such as cities [4]-[5], streets [6] and even universities [7]-[8]. One of the essential components of IoT environment is WSNs [1]. The node in a WSN is classified into a sensor node or a base station (BS) [10]. The sensor nodes are used to collect the surrounding natural events, process data, respond to BS requests and commands or transmit the data to other neighbour sensors. BS (also known as a sink node) mainly sends commands to the sensor nodes to perform particular tasks and receives the collected data from the sensor nodes to perform data aggregation and execute analysis on the collected data [9].

WSNs offer many attributes to encourage sensor deployment over IoT environments, such as low-cost deployment, decentralized nature, soft setting and tearing of the network, multi-hop communication transmission, as well as limited requested resources in terms of energy, processing, memory and communication bandwidth, appealing for more application areas. However, WSNs have more challenges than any other network type in respect to designing efficient security solutions [11]-[15].

Achieving security in WSN applications is very essential, especially in unattended environments and security monitoring applications [16]. Applying security mechanisms to WSN is quite challenging [8], [17]-[18]. This is due to the limited resources of sensor nodes, the nature of communication, the large


1. I. Almomani is with Department of Computer Science, Security Engineering Lab (http://sel.psu.edu.sa/) Prince Sultan University, Riyadh, KSA and with Department of Computer Science, University of Jordan, Amman, Jordan. Email: imomani@psu.edu.sa and i.momani@ju.edu.jo
2. K. Sundus is with Department of Computer Science, University of Jordan, Amman, Jordan. Email: sun.katrina@yahoo.com

and dense sensor node deployment and the dynamic topology of the network [18].

Wireless sensor nodes make WSNs an easy target to different types of attacks, including Denial of Service (DoS) attack due to the open wireless communication and physical risks [19]. To protect WSNs from DoS attacks, we need to ensure the authenticity of the transmitted messages. This could be achieved by applying some Broadcast Authentication (BA) mechanisms to decrease and contain the effect of DoS attacks.

BA is a growing subject in the field of WSN security. BA needs to handle the issue of transmitting messages while receiving other messages in a timely manner, especially in time-sensitive applications. Also, to consider the mobility effect in case of mobile networks [20] to ensure efficient broadcast authentication services. BA allows the BS to broadcast messages to all sensor nodes in the network in a secure manner. Several BA techniques have been proposed to secure WSNs [21]-[22]. However, the mobility of sensors and/or the BS was not taken into consideration. Mobility in WSNs could affect the performance of BA protocols significantly in terms of time delay and energy consumption.

Therefore, this paper investigates the impact of mobility on the behaviour of BAs. Three standard BA protocols; Forwarding First Protocol (FFP), Authentication First Protocol (AFP) and Adaptive Window Protocol (AWP) were implemented and examined against different mobility models. Moreover, FFP, AFP and AWP were evaluated using four main metrics: consumed energy, end-to-end delay, speed and pause time in the presence of different attack intensities. Additionally, four different mobility models were applied to the experimental environment of WSN to test thoroughly the performance of the three BA protocols: fully static WSN, dynamic sensors with static BS, static sensors with mobile BS and fully mobile WSN. The digital signature technique was chosen as a proof of authenticity for the messages transmitted over the network to be able to calculate the processing cost and the amount of consumed energy.

This paper is organized as follows: Section two presents a literature review. Section three summarizes the studied BA protocols and introduces the proposed system architecture. Section four presents the simulation environment, evaluation metrics and the attacking model. Section five presents the simulation results and analysis. Section six draws the conclusion and suggests recommendations for future tasks.

## 2. LITERATURE REVIEW

WSN is a type of wireless network that consists of a large number of resource-constrained sensor nodes and a small number of powerful devices called BS; collaborating together to accomplish a common task by communicating with each other via wireless links [23]. The BS transmits commands or requests to the sensor nodes which could be sent authenticated in some sensitive applications. In general, the security approaches require a certain amount of resources in order to be functional, including data memory, code space and energy to power the sensor nodes [24]. Therefore, the traditional security mechanisms with high computation and communication requirements are undesirable in WSNs and make achieving security a challenging task.

Many security mechanisms in the literature were proposed to protect WSNs against different types of attacks. Patil et al. [18] summarized different existing authentication techniques for WSNs with the main challenges that they are facing in such type of networks. In the following paragraphs, several approaches proposed to achieve broadcast authentication in WSN are discussed.

Timed Efficient Stream Loss-tolerant Authentication (TESLA) and its versions [25]-[26] as well as Digital Signature [27]-[29] techniques were used to implement the BA in WSNs. Furthermore, both techniques protect the entire network from different types of security attacks which assimilate an important role for achieving more trusted messages. In general, the security mechanisms that provide BA in WSNs can be classified into three main categories: Intrusion Prevention-based Systems (IPSs) [23], Intrusion Detection-based Systems (IDSs) [30]-[31] and a combination of both as Intrusion Prevention Detection-based Systems (IPDSs) [32]-[33]. Mittal in [17] summarized the most IDS community that is suitable for WSNs.

Han et al. [34] proposed a key agreement-based authentication technique for dynamic WSNs to decrease the overhead of the authentication process. However, the authors did not provide any simulation experiments to show the efficiency of their proposed approach.

Maidhili et al. [35] proposed an identity-based multi-user BA scheme to provide message authentication. The idea was to minimize the transmission rate to save energy. Moreover, specific authentication techniques were chosen to reduce the computation, but without considering the network mobility.

In [36], the authors proposed BA scheme for smart home. This scheme was based on Elliptic Curve Digital Signature Algorithm (ECDSA) to provide authentication of alarm messages or update messages of service providers in smart home environment. The purpose was to prevent attackers from accessing the home network and injecting forge messages. Another approach which was also based on ECDSA was presented in [37]. This approach supported multiuser BA to preserve both user's privacy and untracking. Both approaches did not consider or evaluate mobility in their proposals.

Shim in [38] proposed an ID-based multiuser BA scheme to minimize computation and communication costs of authentication services in WSNs. The focus was to test the proposed scheme on different hardware platforms, such as MICAz and Tmote Sky, used in real-life deployments. Mobility was not among their evaluation metrics and its effect was not examined.

The work in [39] deployed RSA-like public key cryptography to design a mechanism for multiuser BA in WSNs. The quantitative analyses that the authors conducted showed that their scheme was efficient in terms of storage and computational overheads. But again, there was no consideration for mobility models in their experimental environment.

A bidirectional BA scheme based on Merkle hash tree and TESLA protocol was proposed in [40]. The main idea was adding a verify node in the Merkle hash tree broadcast authentication. This node was responsible to store the entire hash tree. Consequently, their scheme reduced the transmission overhead and ensured secure communications between the central node and the leaf node. Although storage, communication and computation costs were considered in their evaluation and comparison metrics, but mobility effect was also absent in this research.

Applying security techniques in WSNs to achieve message authentication forces the sensor node to perform local operations inside each sensor to verify the correctness of the message, which costs the sensor some of its energy. However, WSN mobility could introduce more overhead on the sensor nodes and could affect the BA protocol performance.

As can be observed from the discussed literature, the current solutions did not highlight how mobility is affecting the performance of authentication services. Therefore, this study investigates the impact of mobility and illustrates to what extent it could affect the performance of broadcast authentication protocols in WSNs.

## 3. AUTHENTICATION PROTOCOLS

This section reviews the three BA protocols studied in this research, in addition to a brief overview about the mobility models in WSNs.

### 3.1 Forwarding First Protocol (FFP)

In FFP protocol [41], the BS sends digitally signed messages. Once the sensors receive these messages, the sensors will forward the messages immediately to the neighbour nodes before checking their validity. In other words, the messages will be forwarded in all cases, regardless of whether the messages are correct or not. After forwarding these messages, the receiver sensors will execute the signature verification processes to ensure the correctness of these messages. If the messages are correct, then the sensor will process the messages. Otherwise, the sensor node will drop the messages after the verification process has failed. As a result, the fake messages are spread across the network. Consequently, sensors' energy is consumed by sending, receiving and verifying fake messages. In general, the transmitted messages contain the index of the message (i), the message itself (M) and the broadcast authenticator of this message ($BA_i$) which is the digital signature in this study. Figure 1 shows the FFP algorithm.

Nevertheless, FFP is usually requested by time-sensitive applications, where the data is transmitted, then verified to avoid any delay of benign messages. However, FFP aids in distributing the malicious messages that deplete the sensors' resources in terms of communication and processing, thus affecting

the overall availability of the entire network.

```
Algorithm 1: Forwarding First Protocol Algorithm
Input: msg ( i, M, BAi )
1: msg = ( i, M, BAi)
2: forward msg;
3: Validity = Check_Broadcast_Authenticator (BAi);
4: if Validity is true Then
5: process the message
6: else                          // Validity is false
7: drop msg;
```

Figure 1. The FFP algorithm.

### 3.2 Authentication First Protocol (AFP)

AFP protocol [41] is another proposed scheme in which the signed messages broadcasted by the BS will be verified first by the sensors before forwarding them to the nearby neighbours. If the messages are correct, the sensor node will forward them, otherwise these messages will be dropped and no forwarding is initiated. Figure 2 shows the AFP algorithm.

```
Algorithm 2: Authentication First Protocol Algorithm
Input: msg ( i, M, BAi )
1:  msg = ( i, M, BAi )
2: Validity = Check_Broadcast_Authenticator (BAi);
3: if Validity is true Then
4: forward msg;
5: else                          // Validity is false
6: drop msg;
```

Figure 2. The AFP algorithm.

AFP limits the scattering of fake messages to only the first hop neighbours of the attackers; hence, farthest nodes will not be affected. In contrast, the delay caused by the verification process of correct messages cannot be neglected.

### 3.3 Adaptive Window Protocol (AWP)

Almomani et al. [42] proposed AWP as a compromising solution between FFP and AFP. AWP uses one-way key chain as a weak pre-authenticator to allow the receiver sensor to recognize the fake messages before verifying their authenticity, thus saving the sensor energy from unnecessary verifications. In other words, AWP provides an indicator whether to apply FFP or AFP in each sensor node. Figure 3 illustrates the AWP algorithm.

As demonstrated in Figure 3, the sensor node first checks the weak pre-authenticator; if it is correct, then each sensor node will check its parameter (W). This W represents the maximum number of hops (H) that the broadcast message can forward without being verified (checking the digital signature). If H >= W, then the node will verify the authenticity of the message. After that, if the message is correctly authenticated, then: (1) it will be forwarded after setting the message's hop counter to zero, indicating that the message has just been authenticated and (2) the window size is progressively updated. Otherwise, the message will be dropped and the window size will be reduced.

Window size is updated according to Equation (1) and Equation (2).

$$cw = \alpha cw + (1 - \alpha)\, AIMD\_W \tag{1}$$

$$w = round(cw) \tag{2}$$

where, *cw* is the current window that is calculated by the AWP, *AIMD_W* is the window size that is computed according to Additive Increase Multiplicative Decrease (AIMD) approach, in which w = ceiling (*w/2*) in case of corrupted message (fake message) and *w = w+1* in case of authentic message (correct message); (w) is the final value which is compared to the hop count value. Additionally, α was chosen to be (0.6) with fake messages and (0.5) with authenticated messages based on experiments.

```
Algorithm 3: Adaptive Window Protocol Algorithm
Input: msg ( i, M, BAi, Ki, H)
1:   msg = ( i, M, BAi, Ki, H)
2:   if Hash(Ki ) = Ki-1 Then // weak pre-authenticator
3:          if H >=W Then   //Authentication first mode
4:                 Validity = Check_Broadcast_Authenticator (BAi);
5:                 if Validity is true Then
6:                        H =0;  // msg = ( i, M, BAi, Ki, H);
7:                        forward msg;
8:                        AIMD_W = cw +1;
9:                        α = 0.5;
10:                else   // Validity is false
11:                       drop msg;
12:                       AIMD_W =cw /2;
13:                       α = 0.6;
14:                end if;
15:         else // H< W
16:                H=H+1;
17:                forward msg;
18:                Validity = Check_Broadcast_Authenticator (BAi);
19:                if Validity is true Then
20:                       AIMD_W = cw +1;
21:                       α = 0.5;
22:                else   // Validity is false
23:                       drop msg;
24:                       AIMD_W = cw / 2;
25:                       α = 0.6;
26:                end if;
27:         end if;
28:         Update w :
29:         cw = α*cw + (1- α)*AIMD_W;
30:         W = round (cw);
31:  else                        // the Ki is not valid in the chain
32:         drop msg;
33:  end if;
34:  Return W;
```

Figure 3. The AWP algorithm [42].

Therefore, the *AIMD_W* upon receiving a corrupted message will take a higher ratio than when receiving an authentic message. These ratios could be changed according to the broadcast nature of the network application and its sensitivity. In case of sensitive applications with high security demands, $\alpha$ should be chosen with small values. The maximum window size (max_win) inside each sensor node is determined with respect to the network size or the sensitivity of the network applications. Eventually, the window size will be generated randomly from the interval [1, max_win] for each sensor node.

### 3.4 Mobility in WSNs

There is a substantial number of mobility models that exist in WSNs. Mobility models are implemented to study the sensor behaviour for different purposes [43]. The dynamic or mobile WSNs (MWSNs) are important due to their major roles in real-world applications. MWSNs are more frequently used than static WSNs [44]-[45]. Additionally, many applications were proposed for mobile base station(s) with a fully static WSN [46]-[47]. Other mobility models could also have a static BS (sink node) and fully dynamic sensor nodes.

Sundus et al. [9] proposed four main mobility models that are considered as the general mobility models; fully static WSN, static sensors with mobile BS network, dynamic sensors with static BS network and fully mobile WSN. These four models were implemented and tested in our study.

### 3.5 System Architecture

Figure 4 shows the system architecture that will be followed in this research. The purpose is to evaluate the three BA protocols under several mobility circumstances and to measure to what extent this could affect the performance of the authentication services. The main performance measures that

were used are the average end-to-end delay of the network and the amount of consumed energy, taking into consideration different network parameters, including attack's intensity, speed and pause time.

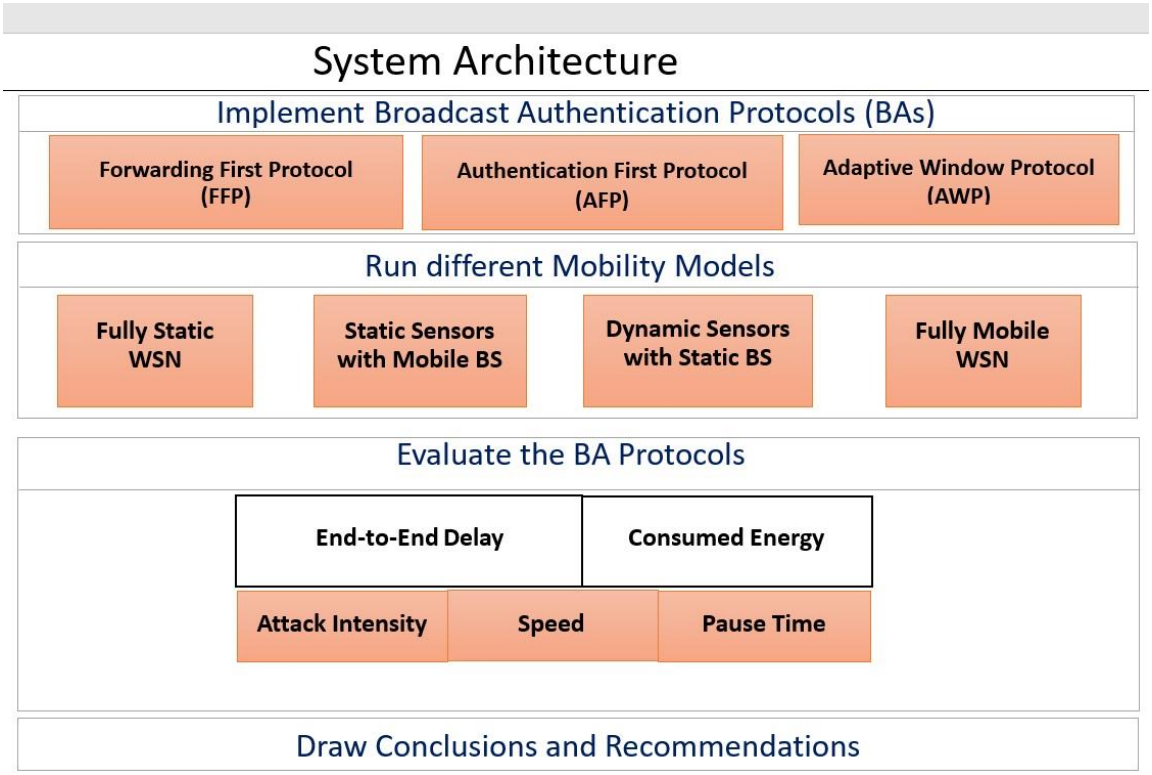



Figure 4. System architecture.

## 4. Simulation Environment and Evaluation Metrics

Simulation experiments were executed to evaluate the impact of mobility on the performance of BA protocols. This section shows the simulation environment, simulation parameters, evaluation metrics and attacking model.

### 4.1 Simulation Environment and Parameters

FFP, AFP and AWP were implemented plus evaluated using Qualnet simulator [48]. The detailed simulation parameters that were used to carry out the scenarios are shown in Table 1.

In the proposed simulation environment, the broadcast messages were sent by the BS to the entire sensor network, *via* multiple hops, where some sensor nodes will forward these messages to the neighbours that are far away from the base station. These broadcast messages are either requests or commands; also, the BS signs the message before sending it. After that, each sensor node may perform the message verification to ensure that the message was sent from the BS (trusted message) and not changed or transmitted by the attacker node.

### 4.2 Evaluation Metrics

The main metrics used to evaluate FFP, AFP and AWP are:

- **Average End-to-end Delay:** This metric analyses the average broadcast delay of the authenticated message in terms of communication and processing time (in seconds) that the message takes until it reaches every node and is processed as well.
- **Average Wasted Energy**: This metric analyses the wasted energy in terms of communication and processing costs (in joules) that is depleted due to injecting the network with fake messages. As a result, the sensor node compels to perform unnecessary operations, such as verifying, sending and receiving these fake messages. Applying security techniques in WSNs to achieve message authenticity requires the sensor node to perform local operations inside

each sensor to verify the correctness of the message, dropping energy from the sensor. Moreover, communication cost is the main source for consuming the sensor's energy.

Table 1. Simulation parameter values.

| Simulation Parameter | Parameter Value |
|---|---|
| Number of BS | 1 Base Station |
| Number of Nodes | 100 nodes |
| Simulation Time | 1250 seconds |
| Network Terrain Size | 1500 meters X 1500 meters |
| Node Placement Model | Randomly |
| Mobility Model | RANDOM-WAYPOINT |
| Mobility Speed | 2.2, 15.5 and 28.8 m/s |
| Mobility Pause Time | 10, 20 and 30 seconds |
| Transport Layer Protocol | UDP |
| Digital Signature | ECDSA-160 |
| Window Size (AWP) | 6 |
| Transmission Range | 250 meters |
| Packet Size | 80 bytes |
| Packet Sending Interval | 30 seconds |
| Routing Protocol | AODV |

- **Attack Intensity:** The purpose of this metric is to examine the behaviour of BA protocols after injecting different intensities of network attackers with different mobile scenarios. Therefore, the attacking model in this research ranges the attack intensity from 0% to 50% of the entire network size.
- **Speed:** Various speeds for mobile nodes were tested using different measurements; meter/second and mile/hour. The approximate mobility speeds are illustrated in Table 2.

Table 2. Approximate mobility speeds.

| Scenario | Speed (mph) | Speed (m/s) |
|---|---|---|
| Walking | 5 | 2.2 |
| City Driving | 35 | 15.5 |
| Free Way Driving | 65 | 28.8 |

- **Pause Time:** The pause time of mobile nodes applied in the simulation scenarios was 0, 10, 20 and 30 seconds, respectively, with node speed set to 15.5 meters per second.

## 4.3 Communication and Processing Costs Analysis

The section provides the analysis for both communication and processing costs in terms of delay and consumed energy.

- ***Communication Delay Analysis***

The communication delay is evaluated in terms of the average time that each message takes to reach the destination, including all possible delays. In other words, the end-to-end delay in mobile WSNs is the time experienced by the message in seconds, which is measured by the generation time of the message at the source node until the message is received by the destination node. In our study, the destination node is every node in the network. The average end-to-end delay for the broadcasting networks [9], [49]-[50] is calculated in Equation (3), where n is the number of messages.

$$\frac{\sum_1^n message\ recieve\ time - message\ sent\ time}{\sum_1^n messages\ recieved} \quad (3)$$

- ***Processing Delay Analysis***

The processing cost is evaluated in terms of the number of signature verifications performed on each message during its trip from the BS until reaching the sensor nodes multiplied by the verification time needed for each verification process which is assumed to be 2 seconds in our study [9], [41]-[42]. In other words, the same signature authentication technique was applied by all analyzed protocols to have fair and accurate results. Equation (4) displays the processing delay analysis.

$$Processing\ Delay = 2 * number\ of\ verifications \quad (4)$$

In more detail, in FFP, each sensor node sends the message before applying the verification process. Thus, after forwarding the message, the verification process is initiated. Hence, the processing delay is not calculated in this protocol. In AFP, each sensor node, before forwarding the message, checks the authenticity of the message first. In case of a fake message, the message will be dropped and the forwarding process will not be initiated. Otherwise, if the message is correct, the message will be forwarded to the next neighbour nodes. AWP is a compromised protocol between FFP and AFP. In this protocol, the most important aspect is the size of the window (which is the number of hops that the message passes without being verified first). Figure 5 shows how delay is changed according to the window size. This study has chosen a window size of 6 to observe the effect of AWP clearly. This window size could be adjusted according to the application sensitivity deployed in WSNs.

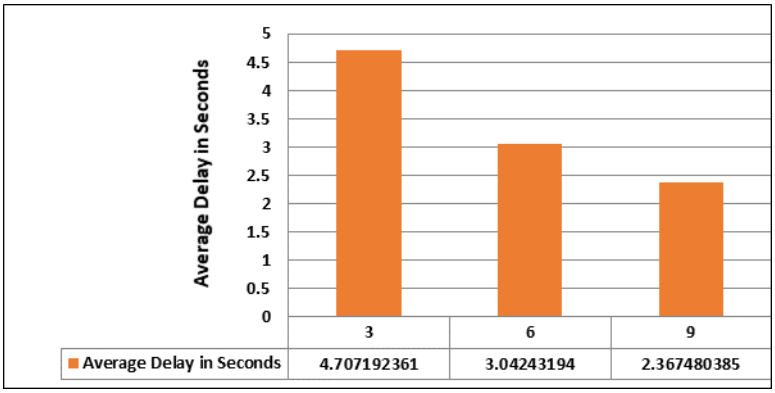



Figure 5. Different window sizes in AWP.

- ***Communication Energy Cost Analysis***

The energy model of the sensor applied in this research is based on the first-order radio model [9], [51]-[55]. Table 3 presents this model.

Table 3. Radio characteristics, first order-radio model [52].

| Radio Model (operation) | Energy Consumption |
|---|---|
| Transmitter Electronics ($E_{Tx-elec}$)<br>Receiver Electronics ($E_{Rx-elec}$)<br>($E_{Tx-elec} = E_{Rx-elec} = E_{elec}$) | 50 nJ/bit |
| Transmit Amplifier ($E_{amp}$) | 100 pJ/bit/m$^2$ |
| Radio Model (operation) | Energy Consumption |

The total wasted energy $T_x$ for transmitting a $k$-bit message is given by Equation (5), where, $k$ is the message size in bits and $d$ is the distance between the sending and the receiving nodes, $E_{elec}$ is the transmitter electronics, $E_{amp}$ is the transmit amplifier. In this study, the average of wasted energy is calculated for retransmitting the fake messages.

$$T_x = E_{elec} * k + E_{amp} * k * d^2 \quad (5)$$

However, $R_x$ is the total wasted energy for receiving a message which is given in Equation (6), whereby $k$ is the received message size in bytes. In this study, the average wasted energy is calculated for receiving fake messages. Therefore, the overall communication cost will be the total amount of

wasted energy for transmitting and receiving fake messages, as shown in Equation (7).

$$Rx = Eelec * k \quad (6)$$

$$\sum Communication\ wasted\ energy = \sum T_x\ (fake\ messages) + \sum R_x\ (fake\ messages) \quad (7)$$

- ***Processing Energy Cost Analysis***

Applying security techniques to any protocol increases the overhead in the network, which consequently increases the depletion of its energy by the verifications executed at each sensor node. Therefore, the processing cost will be the total wasted energy $P_x$ due to fake message verifications, as shown in Equation (8).

$$\sum processing\ wasted\ energy = \sum P_x\ (fake\ messages) \quad (8)$$

Additionally, the security processing cost estimations needed for verifying the messages using different digital signature techniques are measured in milli-Joule [56] and illustrated in Table 4. In this research, we used ECDSA-160 to further examine the variations in the average wasted energy in the three studied protocols.

Table 4. Energy cost estimation for security techniques.

| Digital Signature Techniques | Verification Cost (mJ) |
|---|---|
| RSA-1024 | 14.05 |
| ECDSA-160 | 53.42 |

### 4.4 Attacking Model

If the attacker chooses to affect as many nodes as possible, then the attacker will arrange messages to be transmitted consecutively. Each message created or received by the attacker node will be changed into a fake message and then rebroadcast again.

In FFP, the fake message will be spread throughout the network as there is no review procedure regarding the message before being rebroadcast. Thus, the sensor node as well as the attacker node will rebroadcast the fake messages. Within AFP, sensor nodes close to the attacker would be affected, while sensor nodes far away from the attacker nodes will have limited impact. The fake messages broadcasted from the malicious nodes are dropped by the intermediate nodes. In AWP, sensor nodes close to the attacker will be also affected, but for farther nodes, the impact will be quite limited. Similarly, in AWP, the fake messages are dropped by the intermediate nodes.

## 5. SIMULATION RESULTS AND ANALYSIS

This section illustrates the experimental simulation results of evaluating the three BA protocols using four different mobility models.

### 5.1 Average End-to-end Delay

This sub-section presents the average delay in the BA protocols running at different mobile scenarios and attack intensities.

#### Fully Static Wireless Sensor Network

Figure 6 illustrates the average end-to-end delay in the three protocols against changing the attack intensity. FFP introduces much less amount of average broadcast delay than AFP and AWP; as FFP forwards the message then verifies it. So, there is no consideration regarding message correctness or corruptness. The aim is to forward the message as fast as possible, no matter if the message is trusted or not. On the other hand, AFP has the highest average broadcast delay due to the verification processes that are completed before forwarding the messages again. Therefore, each time the nodes receive a message, the verification process is applied, which delays the message before being rebroadcast again to the next neighbour. AFP ensures that only correct messages will be rebroadcast and fake messages will be dropped. AWP is a compromised protocol between FFP and AFP. When the

attack intensity is high, the window size decreases, which consequently increases the number of verifications. But, when the attack intensity is low or no attackers exist in the network, the window will increase to its maximum size, so the number of verifications will be reduced.

A comparison among the three protocols shows that AWP improved the average delay by up to 80.16% compared to AFP. Also, FFP improved the average delay by up to 94.6% and 98.93% compared to AWP and AFP, respectively.

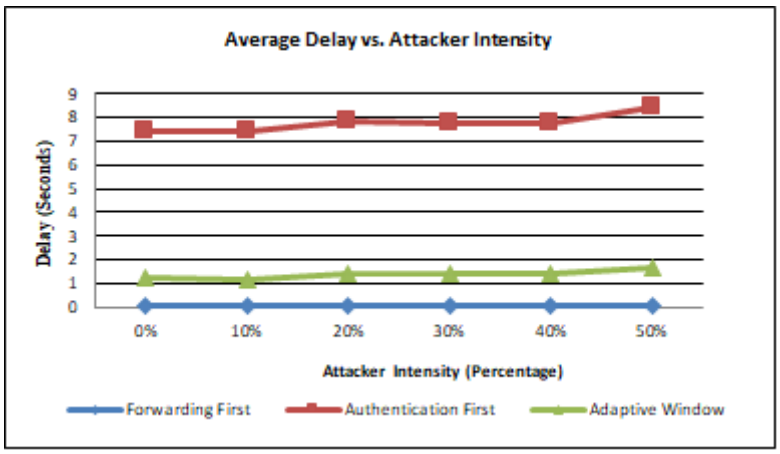



Figure 6. Average delay *vs.* Attacker intensity in static WSN.

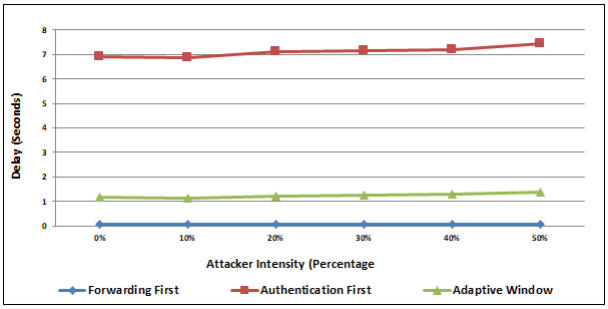
**Static Sensors with Mobile Base Station Network**

Figure 7(a) shows that AWP improved the average delay by up to 81.32% compared to AFP, whereas FFP improved the average delay by up to 93.62% and 98.81% compared to AWP and AFP, respectively. Figure 7(b) illustrates the average end-to-end delay in the three BA protocols when implementing different speeds. In general, the delay decreased after increasing the sensor speed. Figure 7(c) shows the average end-to-end delay after using different pause times. Overall, as pause time increases, the average delay increases as well.

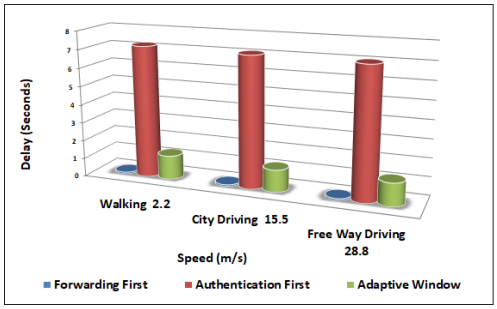
**Dynamic Sensors with Static Base Station Network**

Figure 8(a) illustrates the average end-to-end delay of dynamic sensors with static BS network while changing the attack intensity. As can be observed, AWP improved the average delay by up to 88.24% compared to AFP, whereas FFP improved the average delay by up to 85.63% and 98.31% in comparison with AWP and AFP, respectively.

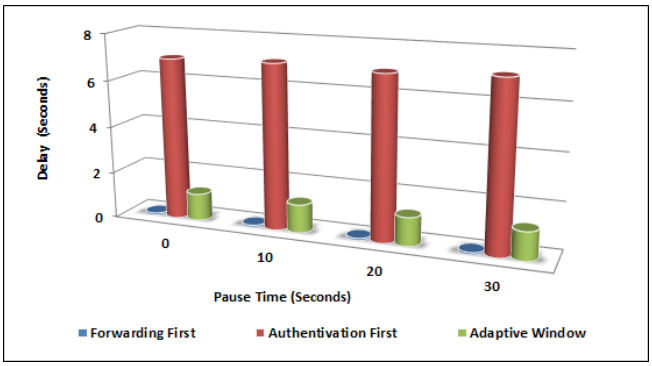
Figure 8(b) illustrates the average end-to-end delay in the three protocols after applying different speeds. The average delay time in FF protocol decreased by 15.9% due to speed increase. In regard to AFP and the AWP, fewer message loss has occurred, since they allotted time for the verification process before sending out the messages again, consequently giving the sensor node time to locate other viable connections. Further, the average delay increased by up to 63.3% and 73.5% in both AFP and AWP, respectively when there is a boost in speed.




(a) Average delay vs. Attacker intensity
Speed = 15 Pause time = 30



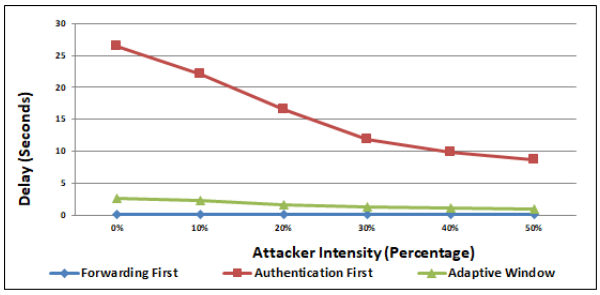

(b) Average delay vs. Speed
Pause time = 30 Attacker intensity = 20%



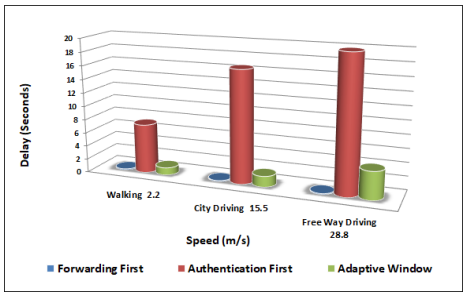

(c) Average delay vs. Pause time,
Speed = 15 Attacker intensity

Figure 7. Average end-to-end delay in static sensors with mobile BS network.

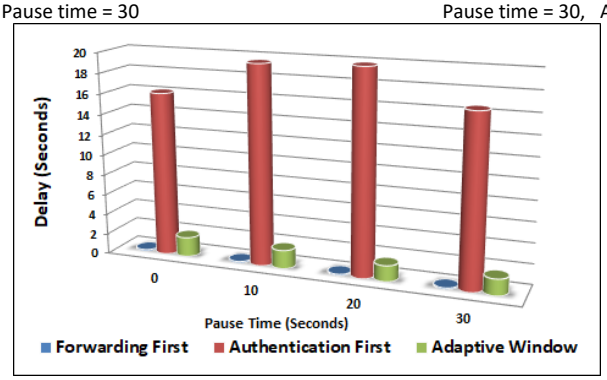
Figure 8(c) illustrates the decrease in FFP and AWP delay by 7.1% and 16.4%, respectively after increasing the pause time. However, AFP's average delay increased by up to 18.7% until the pause time reached 20, then the average delay decreased.




(a) Average delay vs. Attacker intensity
Speed =15 Pause time = 30




(b) Average delay vs. Speed
Pause time = 30, Attacker intensity = 20%




(c) Average delay vs. Pause time
Speed = 15 Attacker intensity = 20%

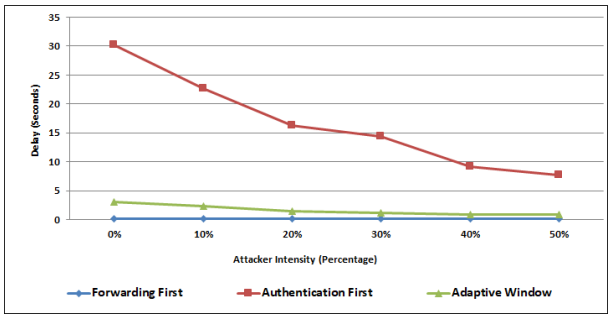
Figure 8. Average end-to-end delay in dynamic sensors with static BS network.

### A Fully Mobile Wireless Sensor Network

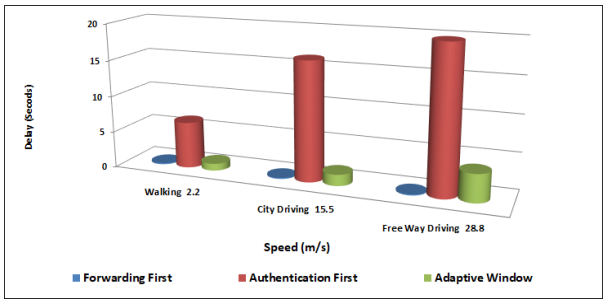
Figure 9(a) shows the improved delay of AWP over AFP by up to 88.67%, whereas FFP outperformed both AWP and AFP by improving the delay by 83.15% and 98.1%, respectively, considering different attack intensities.

Figure 9(b) illustrates the average delay at different speed values in fully mobile WSN. FFP decreased the average delay by 16.9% while increasing the speed. However, AFP and AWP introduced more delay due to message verification before message forwarding. Thus, AFP and AWP average delay had an increase of 74.38% and 67.68%, respectively during a speed increase.

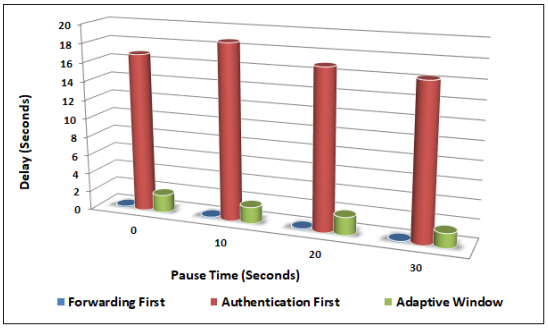
Figure 9(c) illustrates the average end-to-end delay using different pause times. FFP had an average delay that decreased by 6.8%. However, AFP's delay increased by up to 9.7% until the pause time reached 10, then it was decreased by 12.6%. Moreover, in both AWP and AFP, the delay increased by up to 9% until the pause time reached 20, then it was decreased by 19.1%.




(a) Average delay vs. Attacker intensity
Speed = 15 Pause time 30




(b) Average delay vs. Speed
Pause time = 30 Attacker intensity = 20%




c) Average delay vs. Pause time
Speed = 15 Attacker intensity

Figure 9. Average end-to-end delay in fully mobile WSN.

## 5.2 Average Wasted Energy

In this sub-section, the BA protocols are evaluated in terms of wasted energy, considering different mobility models, attack intensities, speeds and pause times.

### Fully Static Wireless Sensor Network

Figure 10 shows the average wasted energy after forwarding, receiving and verifying fake messages produced by the three protocols under various attack intensities. Comparing the behaviours of FFP, AFP and AWP, it can be observed that the average wasted energy consumed by AWP is small-scale compared to FFP and AFP. The reason is that AWP depends on verifying the weak pre-authenticator each time before forwarding the message. As a result, the AWP discovers fake messages before verifying the broadcast authenticator (digital signature) and stops spreading the fake messages over the network. As can be observed, AFP wasted energy by up to 84.2% less than FFP, whereas AWP wasted energy by up to 65% and 94.4% less than AFP and FFP, respectively.

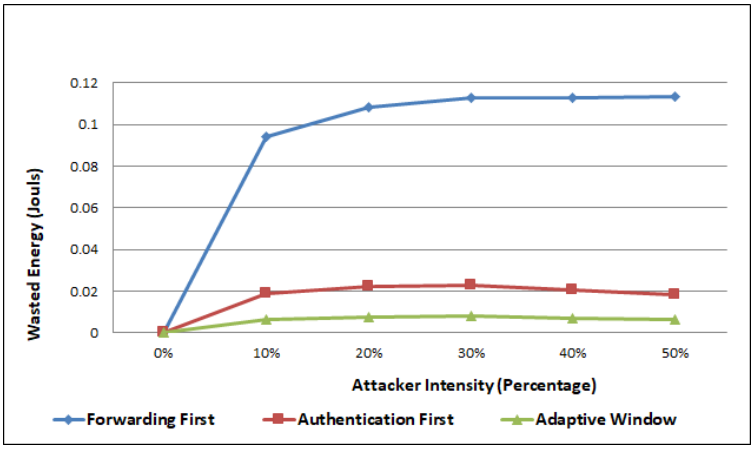



Figure 10. Average wasted energy *vs.* attack intensity in static WSN.

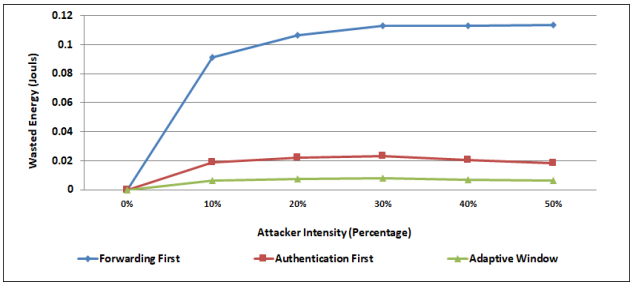
### Static Sensors with Mobile Base Station

Figure 11(a) illustrates the average wasted energy in the three protocols while changing the attack

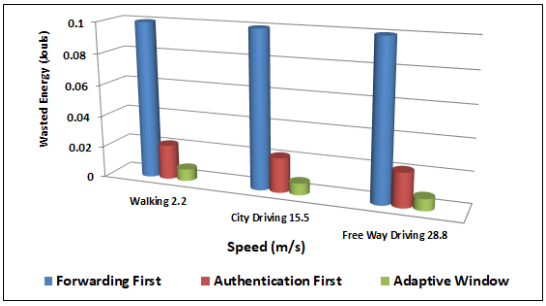
intensity. AFP wasted up to 84.04% less energy than FFP. AWP wasted up to 65.5% and 94.5% less energy than AFP and FFP, respectively.

Figure 11(b) shows the average wasted energy produced under different speeds. The results revealed that FFP, AFP and AWP have an energy consumption decrease by 2.02%, 94.5% and 2.8%, respectively during the speed increase. In general, having static sensors with mobile BS network, the average wasted energy slightly decreased while increasing the speed.

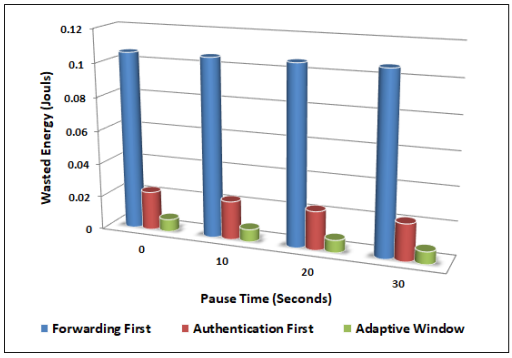
Figure 11(c) shows the average wasted energy under different pause times. Comparing the behaviours of FFP, AFP and AWP, it can be noted that the three tested protocols relatively stayed the same, although different pause times were adopted. FFP, AWP and AFP had an energy consumption increase by up to 0.55%, 0.96% and 4.28%, respectively during the increase of pause time. In general, the average wasted energy slightly increases as the pause time increases.




(a) Average wasted energy vs. Attacker intensity
Speed = 15 Pause = 30




(b) Average wasted energy vs. Speed
Pause time = 30 Attacker intensity = 20%



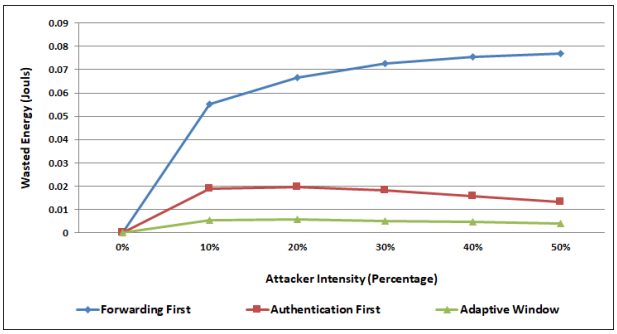

(c) Average wasted energy vs. Pause time
Speed = 15 Attacker intensity = 20%

Figure 11. Average wasted energy in a static sensors and mobile BS network.

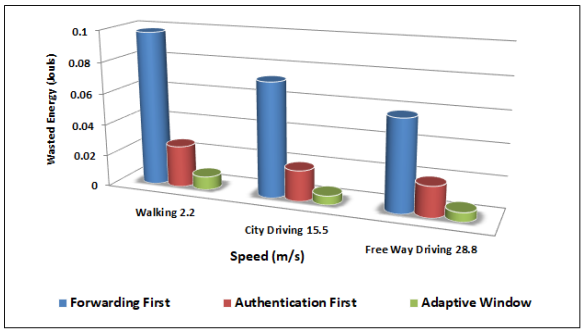
## Dynamic Sensors with Static Base Station Network

Figure 12(a) illustrates the average wasted energy when changing the attack intensity. AFP wasted energy reached 82.58% less than FFP, whereas AWP wasted energy by up to 70.4% and 94.8% less than AFP and FFP, respectively.

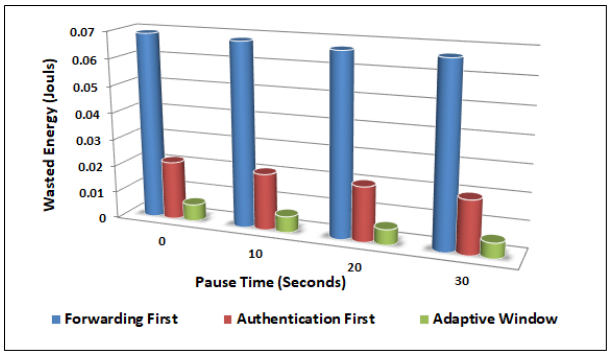
Figure 12(b) displays the average wasted energy spent in processing and communicating fake




(a) Average wasted energy vs. Attacker intensity
Speed = 15 Pause time = 30




(b) Average wasted energy vs. Speed
Pause time = 30 Attacker intensity = 20%




(a) Average wasted energy vs. Pause time
Speed = 15 Attacker intensity = 20%

Figure 12. Average wasted energy in a dynamic sensors with static BS network.

messages produced by the three protocols under different speeds. As can be seen, the energy consumption decreased by 41.02%, 26.53% and 31.57% during speed increase in FFP, AFP and AWP, respectively.

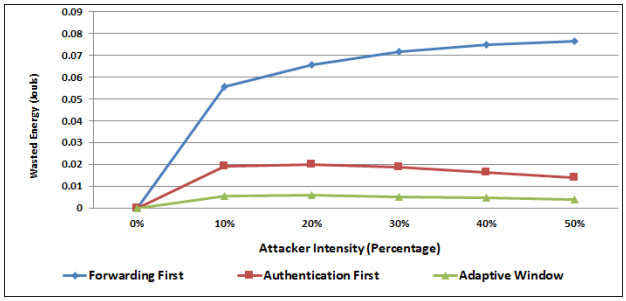
Figure 12(c) illustrates the average wasted energy while applying different pause times. FFP, AFP and AWP consumed energy increased by 3.3%, 8.44% and 8.49%, respectively during long pause times. This is due to receiving additional fake messages from the sensor nodes due to long pause times.

**Fully Mobile Wireless Sensor Network**

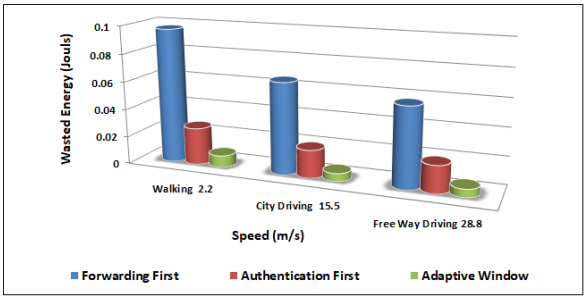
Figure 13(a) illustrates the average wasted energy against attack intensity. AFP wasted energy reached 82.13% less than FFP. Also, AWP wasted energy reached 70.65% and 94.76% less than AFP and FFP, respectively.

Figure 13(b) demonstrates that the average wasted energy decreased by 41.1%, 26.9% and 32.2% in FFP, AFP and AWP, respectively during speed increase.

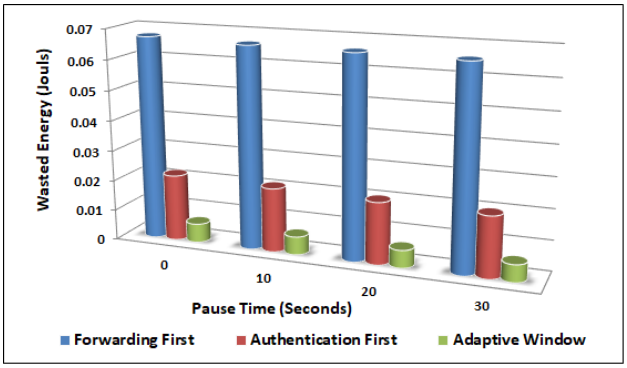
Figure 13(c) shows the average wasted energy caused by the three protocols under different pause times. FFP, AFP and AWP energy consumption decreased by 2.3%, 8.6% and 7.75%, respectively after increasing the pause time.




(a) Average wasted energy vs. Attacker intensity
Speed = 15 Pause time = 30




(b) Average wasted energy vs. Speed
Pause Time = 30 Attacker intensity = 20%




(c) Average wasted energy vs. Pause time
Speed = 15 Attacker intensity = 20%

Figure 13. Average wasted energy in a fully mobile WSN.

### 5.3 Summary of Results

Table 5 shows the average delay and the average wasted energy values for FFP, AFP and AWP in all mobility models against 30% attack intensity. This is to facilitate the comparison among the three protocols at a specific attack intensity. The order of protocols in terms of causing less delay in WSN was FFP, AWP and then AFP. In terms of protocols with less consumed energy, the order was AWP, AFP and then FFP, respectively. The differences among these protocols can be observed in Table 5.

Table 5. Average delay and wasted energy for the studied protocols with 30% attack intensity.

| The Studied Protocols | Static WSN | | Mobile BS with Static WSN | | Static BS with Mobile WSN | | Fully Mobile WSN | |
|---|---|---|---|---|---|---|---|---|
| | Wasted Energy | Delay | Wasted Energy | Delay | Wasted Energy | Delay | Wasted Energy | Delay |
| **FFP** | 0.11268760 | 0.09012260 | 0.11295186 | 0.08858713 | 0.07263590 | 0.14543172 | 0.07155085 | 0.14668910 |
| **AFP** | 0.02299114 | 7.79333621 | 0.02299347 | 7.16931291 | 0.01816784 | 11.9163161 | 0.0185301 | 14.447714 |
| **AWP** | 0.00804712 | 1.39683641 | 0.00800553 | 1.26098829 | 0.00523681 | 1.28649027 | 0.0052342 | 1.1477775 |

To provide more comprehensive results, Table 6 summarizes the comparison among FFP, AFP and AWP, where each protocol is compared with itself in case of fully static WSN and when mobility exists. This is to illustrate how the performance of a specific protocol could be affected after introducing mobility. Both FFP and AFP performances were the best in case of mobile BS with static sensors and fully mobile WSN in terms of delay and wasted energy, respectively. On the other hand, AFP performed the best in case of fully mobile WSN and static BS with mobile sensors in terms of delay and wasted energy, respectively. Overall, the best improvements in terms of delay and wasted energy were observed in AWP in comparion with the other two BA protocols.

Table 6. Comparison between each protocol in a fully static WSN with itself using different mobility models.

| The Studied Protocols | Mobile BS with Static WSN | | Static BS with Mobile WSN | | Fully Mobile WSN | |
|---|---|---|---|---|---|---|
| | Wasted Energy | Delay | Wasted Energy | Delay | Wasted Energy | Delay |
| **FFP** | 0.27% more | 1.7% less | 31.97% less | 38% more | 32.3%less | 38.5% more |
| **AFP** | 0.14% more | 11.3% less | 25.8% more | 2.45% more | 24.4% less | 8.37% less |
| **AWP** | 1.33% less | 16.5% less | 37.3% less | 13.2% more | 36.6% less | 47.6% less |

## 6. CONCLUSIONS

Authentication is an important security requirement that needs to be enforced in WSNs. Authentication ensures correct communication between the Base Station (BS) and the sensor nodes. The request or command sent by the BS should be authentic, as it controls the functionality of the WSN and its provided services.

This research examined the effect of mobility on different authentication approaches; the Forwarding First Protocol (FFP), the Authentication First Protocol (AFP) and the Adaptive Window Protocol (AWP) protocols. The performances of FFP, AFP and AWP were experimented against four mobility models: fully static WSN, static sensors with mobile BS, dynamic sensors with static BS network and fully mobile WSN and were measured using different evaluation metrics, including consumed energy, end-to-end delay, speed and pause time.

The simulation results demonstrated that the behaviour of the three BA protocols, which experienced several mobility scenarios, has stayed essentially consistent with differences in the average broadcast delay and the average wasted energy. The average broadcast delay was the best in FFP, but this protocol was the worst in terms of consumed energy. On the other hand, AWP was the best in terms of average wasted energy. Therefore, it can be concluded that AWP was the best protocol in terms of average broadcast delay and average wasted energy, especially when the network is under attack.

For future work, other BA protocols could be tested against mobility models. Also, since the behaviour of protocol has changed in response to mobility, a smart protocol could be designed to flip from one authentication technique to another to maintain efficient authentication services in WSNs.

## REFERENCES

[1] B. Mbarek, A. Meddeb, W. Ben Jaballah and M. Mosbah, "A Broadcast Authentication Scheme in IoT Environments," Proc. of the 13th IEEE International Conference of Computer Systems and Applications (AICCSA), Dec. 2016.

[2] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari and L. Wu, "A Lightweight and Robust Two-factor Authentication Scheme for Personalized Healthcare Systems Using Wireless Medical Sensor Networks," Future Generation Computer System, vol. 82, pp. 727-737, 2018.

[3] Th. Arampatzis, J. Lygeros and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," Proc. of the 13th Mediterranean Conference on Control and Automation, pp. 719-724, 2005.

[4] O. B. Mora, R. Rivera, V. M. Larios, J. R. Beltrán-Ramírez, R. Maciel and A. Ochoa, "A Use Case in Cybersecurity Based in Blockchain to Deal with the Security and Privacy of Citizens and Smart Cities Cyberinfrastructures," IEEE International Smart Cities Conference (ISC2), Sept. 2018.

[5] A. Founoun and A. Hayar, "Evaluation of the concept of the smart city through local regulation and the importance of local initiative", IEEE International Smart Cities Conference (ISC2), USA, Sept. 2018.

[6] P.-A. Mohandas, J. S. A. Dhanaraj and X.-Z. Gao, "Artificial Neural Network based Smart and Energy Efficient Street Lighting System: A Case Study for Residential Area in Hosur," Elsevier, Sustainable Cities and Society, vol. 48, July 2019.

[7] D. J. A. Lewis, "The SMART University: The Transformational Role of Learning Analytics," Information and Learning Science, vol. 119, no. 12, pp. 758-760, 2018.

[8] H. Sharma and G. Kaur, "Optimization and Simulation of Smart Grid Distributed Generation: A Case Study of University Campus," IEEE Smart Energy Grid Engineering (SEGE), Aug. 2016.

[9] K. Sundus and I. Almomani, "Mobility Effect on the Authenticity of Wireless Sensor Networks," Proc. of IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, April 2019.

[10] H. Singh and D. Singh, "Taxonomy of Routing Protocols in Wireless Sensor Networks: A Survey," Proc. of the 2nd International Conference on Contemporary Computing and Informatics (IC3I), pp. 822-830, 2016.

[11] I. Almomani and M. Saadeh, "FEAR: Fuzzy-based Energy Aware Routing Protocol for Wireless Sensor Networks," International Journal of Communications, Networks and System Sciences, vol. 4, no. 6, pp. 403-415, June 2011.

[12] M. Kocakulak and I. Butun, "An Overview of Wireless Sensor Networks towards Internet of Things," Proc. of the 7th IEEE Annual Computing and Communication Workshop and Conference (CCWC), pp. 1-6, 9-11 January 2017.

[13] P. Rawat, K. D. Singh, H. Chaouchi and J. M. Bonnin, "Wireless Sensor Networks: A Survey on Recent Developments and Potential Synergies," Journal of Supercomputing, vol. 68, no. 1, pp. 1–48, April, 2014.

[14] S. K. Gupta and P. Sinha, "Overview of Wireless Sensor Network: A Survey," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 1, pp. 5201-5207, Jan. 2014.

[15] M. R. Ahmed, X. Huang, D. Sharma and H. Cui, "Wireless Sensor Networks: Characteristics and Architectures," International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, vol. 6, no. 12, pp. 1398-1401, 2012.

[16] W. B. Jaballah, M. Mosbah, H. Youssef and A. Zemmari, "Lightweight Secure Group Communications for Resource Constrained Devices," International Journal of Space- based and Situated Computing, vol. 5, no. 4, pp. 187-200, 2015.

[17] N. K. Mittal, "A Survey on Wireless Sensor Network for Community Intrusion Detection Systems," Proc. of the 3rd IEEE Int'l Conf. on Recent Advances in Information Technology, 2016.

[18] S. Patil, V. Kumar B. P., S. Singh and R. Jamil, "A Survey on Authentication Techniques for Wireless Sensor Networks," International Journal of Applied Engineering Research, vol. 7, no.11, 2012.

[19] B. Mbarek, A. Mddeb, W. Ben Jaballah and M. Mosbah, "An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks," Procedia Computer Science, vol. 109C, pp. 553-559, 2017.

[20] K. Grover and A. Lim, "A Survey of Broadcast Authentication Schemes for Wireless Networks," ELSEVIR *Ad Hoc* Networks, Part A, vol. 24, pp. 288-316, January 2015.

[21] M. Jan, P. Nanda, M. Usman and X. He, "Pawn: A Payload-based Mutual Authentication Scheme for Wireless Sensor Networks," Concurrency and Computation: Practice and Experiance, vol. 29, no. 17, 2016.

[22] V. Khanaa, K. Thooyamani and R. Udayakumar, "A Secure and Efficient Authentication System for Distributed Wireless Sensor Network," World Applied Science Journal (Computer Sceince, Engineering and Its Applications), pp. 304-308, 2014.

[23] I. Almomani and M. Alenezi, "Efficient Denial of Service Attacks Detection in Wireless Sensor Networks," Journal of Information Science and Engineering, vol. 34, no. 4, pp. 977-1000, 2018.

[24] J. P. Walters, Z.-Q. Liang, W.-S. Shi and V. Chaudhary, "Wireless Sensor Network Security: A Survey," Security in Distributed, Grid and Pervasive Computing, p. 367, 2006.

[25] H. Huang, T. Gong, T. Chen, M.-L. Xiong, X.-X. Pan and T. Dai, "An Improved $\mu$ TESLA Protocol Based on Queuing Theory and Benaloh-Leichter SSS in WSNs," Journal of Sensors, p. 13, 2016.

[26] M. R. Kumar and C. S. G. Dhas, "An Analysis of Broadcast Authentication and Security Schemes in Wireless Sensor Networks," International Journal of Engineering and Technology (IJET), vol. 5, no. 5, pp. 3992-4001, Nov. 2013.

[27] B. Bezawada, S. Kulkarni and I. Ray, "Independent Key Distribution Protocols for Broadcast Authentication," Symposium on Access Control Models and Technologies (SACMAT 18), pp. 27-38, 13-15 June 2018.

[28] R. Ali, A. K. Pal, S. Kumari, M Karuppiah and M. Conti, "A Secure User Authentication and Key-agreement Scheme Using Wireless Sensor Networks for Agriculture Monitoring," Future Generation Computer Systems, vol. 84, pp. 200-2015, 2018.

[29] S. Challa, A. Kumar Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan and A. V. Vasilakos, "An Efficient ECC-based Provably Secure Three-factor User Authentication and Key Agreement Protocol for Wireless Healthcare Sensor Networks," Computers and Electrical Engineering, vol. 69, pp. 534-554, July 2018.

[30] C. Ioannou, V. Vassiliou and C. Sergiou, "An Intrusion Detection System for Wireless Sensor Networks," Proc. of the 24th International Conference on Telecommunications (ICT), 3-5 May 2017.

[31] I. Butun, S. D. Morgera and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, pp. 266 - 282, May 2013.

[32] Krontiris, Intrusion Prevention and Detection in Wireless Sensor Networks, PhD Thesis, Naturwissenschaften der Universit¨at Mannheim, Mannheim, 2008.

[33] O. Karajeh, Securing Wireless Sensor Networks Against Denial of Service Attacks, Thesis for the Master's Degree of Computer Science, 2010.

[34] K. Han and T. Shon, "Sensor Authentication in Dynamic Wireless Sensor Network Envionments," International Journal of RFID Security and Cryptography (IJRFIDSC), vol. 1, no. 1/2, 2012.

[35] R. Maidhili and G. M. Karthik, "Energy Efficient and Secure Multi-user Broadcast Authentication Scheme in Wireless Sensor Networks," Proc. of IEEE International Conference on Computer Communication and Informatics (ICCCI), Jan. 2018.

[36] D.-H. Lee and I.-Y. Lee, "ECDSA-based Broadcast Authentication Scheme for Smart Home Environments," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 10, no. 4, pp. 81-86, 2018.

[37] H. Bashirpour, S. Bashirpour, S. Shamshirband and A. Chronopoulos, "An Improved Digital Signature Protocol to Multi-user Broadcast Authentication Based on Elliptic Curve Cryptography in Wireless Sensor Networks (WSNs)," Mathematical and Computational Applications, vol. 23, no. 2, pp.17, 2018.

[38] K.-A. Shim, "BASIS: A Practical Multi-user Broadcast Authentication Scheme in Wireless Sensor Networks," IEEE Trans. on Information Forensics and Security, vol. 12, no. 7, pp. 1545-1554, 2017.

[39] C.-Y. Cheng, I.-C. Lin and S.-Y. Huang, "An RSA-like Scheme for Multiuser Broadcast Authentication in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 11, no. 9, A. ID. 743623, pp. 1-11, 2015.

[40] L. Xu, M. Wen and J. Li, "A Bidirectional Broadcasting Authentication Scheme for Wireless Sensor Networks," Proc. of IEEE Conference on Collaboration and Internet Computing (CIC), pp. 200-204, 2015.

[41] W. Ronghua, D. Wenliang and N. Peng, "Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks," Proceedings of the 8th ACM International Symposium on Mobile *Ad Hoc* Networking and Computing, pp. 71-79, 2007.

[42] I. Almomani, O. Karajeh and L. Abdullah, "Reducing the Vulnerability of Broadcast Authentication against Denial of Service Attacks in Wireless Sensor Networks," The Mediterranean Journal of Computer and Networks, vol. 7, no. 2, 2011.

[43] V. Ramasamy, "Mobile Wireless Sensor Networks: An Overview," Wireless Sensor Networks, [Online], Available: https://www.intechopen.com/books/wireless-sensor-networks-insights-and-innovations/mobile-wireless-sensor-networks-an-overview, October 4th, 2017.

[44] S. M. Mohamed, H. S. Hamza and I. A. Saroit, "Coverage in Mobile Wireless Sensor Networks (M-WSN): A Survey," Computer Communications, vol. 110, pp. 133-150, 15 September 2017.

[45] J. Rezazadeh, M. Moradi and A. S. Ismail, "Mobile Wireless Sensor Networks Overview," International Journal of Computer Communications and Networks (IJCCN), vol. 2, no. 1, February 2012.

[46] N. Ghosh and I. Banerjee, "Application of Mobile Sink in Wireless Sensor Networks," Proc. of the 10th International Conference on Communication Systems & Networks (COMSNETS), 3-7 Jan. 2018.

[47] P. Zhong and F. Ruan, "Application of Mobile Sink in Wireless Sensor Networks Study on the Effect of Sink Moving Trajectory on Wireless Sensor Networks," Proc. of IOP Conference Series: Materials Science and Engineering, vol. 323, 2018.

[48] Scalable Network Technologies, "Qualnet 5.0, Qualnet Network Simulator," [Online], Available: https://www.scalable-networks.com/qualnet-network-simulation.

[49] L. Kumar, "Scalability Performance of AODV, TORA and OLSR with Reference to Variable Network Size," International Journal of Engineering Research and Applications (IJERA), vol. 2, pp. 87-92, 2012.

[50] T. Javed and S. Zafar, "Delay Analysis of Manet Routing Protocols," World Applied Science Journal, vol. 19, no. 5, pp. 615-520., 2012.

[51] J. Banerjee, S. K. Mitra and M. K. Naskar, "Comparative Study of Radio Models for Data Gathering in Wireless Sensor Networks," International Journal of Computer Applications, vol. 27, no. 4, 2011.

[52] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks," Proceeding of the 33rd IEEE Annual Hawaii International Conference on System Science, vol. 2, no. 10, 2000.

[53] H. Aljawawdeh, I. Almomani, "Dynamic load balancing protocol (DLBP) for wireless sensor networks", IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), pp. 1–6, 3-5 Dec. 2013.

[54] H. G. Goh, M. L. Sim and H. T. Ewe, "Energy Efficient Routing for Wireless Sensor Networks with Grid Topology," International Federation for Information Processing (IFIP), pp. 834-843, 2006.

[55] I. Almomani, M. Saadeh, M. AL-Akhras, and H. AL Jawawdeh, “A Tree-Based Power Saving Routing Protocol for Wireless Sensor Networks”, International Journal of Computers and Communications, Vol. 5, no. 2, pp. 84-92, 2011.

[56] I. Almomani and M. Saadeh, "Security Model for Tree-based Routing in Wireless Sensor Networks: Structure and Evaluation," KSII Transactions on Internet and Information Systems (TIIS), vol. 6, no. 4, pp. 1223-1247, 2012.

Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 06, No. 01, March 2020.

**ملخص البحث:**

إن تطبيقات شبكات المجسّات اللاسلكية تتمتع بأهمية كبيرة هذه الأيام، وهي منتشرة في العديد من جوانب حياتنا. وتعدّ بروتوكولات التحقق من أصالة البث حلولاً لضمان أن الأوامر والطلبات التي ترسلها المحطة الأساسية التي تتحكم في الخدمات المقدمة من شبكة المجسات اللاسلكية، هي أوامر وطلبات أصليه. وتعدّ حركية الشبكة أحد التحديات الأساسية التي تواجهها خدمات هذا النوع من الشبكات بشكل عام وبروتوكولات التحقق من الأصالة على وجه الخصوص؛ إذ إن البروتوكولات المتوافرة حاليا للتحقق من الأصالة لم تتفطّن كثيراً الى أثر المحطة الأساسية المتحركة و/أو المجسات المتحركة في سلوك تلك البروتوكولات.

وعليه، تقدم هذه الورقة تحليلاً معمَّقاً لأثر الحركيّة في سلوك بروتوكولات التحقق من أصالة البثّ. وقد تمت دراسة ثلاثة تصاميم مرجعية لبروتوكولات التحقق من أصالة البثّ، هي: التمرير أولاً، والتحقق من الأصالة أولاً، والنافذة التكيفية. وجرى فحص هذه البروتوكولات الثلاثة مقابل أربعة نماذج رئيسية للحركيّة. وكشفت النتائج أنّ بروتوكولات التحقق من أصالة البثّ تصرّفت على نحوٍ مختلف من حيث استهلاك الطاقة والتأخير في الشبكة في وجود الحركية. فعلى سبيل المثال، كان التأخير في بروتوكول النافذة التكيفية قد انخفض بنسبة 47.6% في حالة شبكة المجسات اللاسلكية المتحركة بالكامل، بينما انخفض فقْد الطاقة بنسبة 37.5% في حالة المحطة الأساسية الثابتة والمجسات المتحركة. وعلى الرغم من استخدام تقنية التحقق من الأصالة نفسها للبروتوكولات الثلاثة، فإنّ الحركيّة كانت في حدّ ذاتها سبباً في تحسين الأداء أو تدهوره فيما يتعلق بخدمة التحقق من الأصالة؛ الأمر الذي يؤثر بدوره في أمان شبكات المجسات اللاسلكية والخدمات التي توفرها. فعلى سبيل المثال وفي حالة وجود محطة أساسية متحركة ومجسات ثابتة ، فقد عمل بروتوكول التمرير أولاً على إنقاص التأخير في الشبكة بنسبة وصلت الى 98.81% مقارنة ببروتوكولات التحقق من الأصالة أولاً وبنسبة وصلت الى 93.62% مقارنة ببروتوكول النافذة التكيفية. من جهة أخرى، عمل بروتوكول النافذة التكيفية على توفير طاقة الشبكة بنسبة وصلت الى 94.49% مقارنة ببروتوكول التمرير أولاً وبنسبة وصلت الى 65.5% مقارنة ببروتوكول التحقق من الأصالة أولاً.