A Cybersecurity Model for the Enhancement of WiMAX-based Wireless Communications Infrastructure to Serve Smart Grid Applications

Firas S. Alsharbaty *‡, Qutaiba I. Ali **

* Department of Electrical, Engineering college, University of Mosul

** Department of Computer, Engineering college, University of Mosul

(alsharbaty@uomosul.edu.iq, Qut1974@gmail.com)

‡Corresponding Author; Firas S. Alsharbaty

alsharbaty@uomosul.edu.iq

Received: xx.xx.xxxx Accepted:xx.xx.xxxx

Abstract- This research paper addresses on a secured wireless communications network (WCN) based on WiMAX infrastructure for smart grid applications. The proposed infrastructure consists of WiMAX base stations (BSs) enhanced by edge computing to assimilate the various types of smart grid applications (real time applications and non-real time applications) like wide area monitoring and control (WAMC), video surveillance, tariffs, alarm, and demand side management (DSM). The current work adopts a robust cybersecurity model for the suggested WCN and discusses the possible threats and attacks on the security model. The results indicated that, the WCN based on decentralized processing and self-powered can handle the adopted applications of smart grid successfully. Further, the results explained that the ciphering technique of cybersecurity model does not break the requirements of real time applications' system performance in terms of latency and received data reliability.

Keywords: Advanced metering infrastructure (AMI), Cybersecurity, Real time applications, Smart grid, WiMAX.

1. Introduction

In general, the communications network infrastructure of the smart grid is a wide area network which suffers from high-cost initialization, maintenance, and rigidity. WiMAX technology is a wireless metropolitan area network (WMAN) offering a package of features like long coverage area, respected capacity, and flexibility. However, the employing of wireless access networks faces some challenges related to the power consumption of BSs in the cellular system and the preferable sites to initialize the BSs of such systems [1]. Further, the issues of cybersecurity increase in the wireless channel such as unauthorized access and malicious access attempts [2] [3].

On the other side, the smart grid network involves in huge number of different types of data sources and many kinds of applications producing heavy data traffic. In this sense, the communication network of smart grid should be handled the obstacles in terms of power consumption, data processing, and resilience.

In the literatures, the work in [4] investigated the reliability and topology of the wireless communications network of the smart grid in the case of dealing with AMI applications. While the work in [5] studied the possibility of exploiting the Internet in term of WCN for smart grid applications where the mentioned work adopted testbed based on one way communication to measure the latency of some wireless technologies.

Other previous works adopted WiMAX technology to design communications network infrastructure to serve the applications of smart grid. However, the works in [6] and [7] built an AMI Network infrastructure based on one WiMAX BS for limited number of users in term of smart meters. These works analysed the results of AMI applications in term of delay based-type of service. In the same context, the works in [8], [9] and [10] designed WiMAX network infrastructure to support more clients compared to the previous mentioned works in term of SMs and estimated the coverage area of BS under the nominal wireless channel. Whilst, the attitude of the work in [11] paid attention to exploit WiMAX system to design a wide area network to connect multi–Phasor Measurement Units (PMUs) to the control center of the power grid to deal with WAMC applications. The authors dedicated their infrastructure to handle one type of applications. Other works such as [12] [13] [14] and [15] presented the cloud computing to process the data at the control center of the smart grid.

In term of cybersecurity, there are dearth of related works that dealt with the security in the wireless networks for smart grid applications. Hence, the most of related works

in this field address the security issues in term of review papers or handling the security in wired technologies.

However, the absence of addressing vital points in an integrated work is concluded from the previous related works such as the wireless communications network infrastructure for wide area network should assimilate various smart grid applications from resilience, data processing, real time latency, and data reliability points of view. As well, the issue of cybersecurity in the area of wireless technologies and the vital infrastructure requires handling and taken into consideration.

With the intention of address the previous subjects, the current work presents the following contributions: This work suggests WCN infrastructure of smart grid addressing self-powered based on renewable energy to mitigate the burden on the power grid, and it engages with distributed data processing based on edge computing in a wireless fashion to handle the distributed environment of smart grid, data reliability, small latency, and assimilate the heavy data traffic points of view. Furthermore, after introducing the possibly threats and attacks for the WCN based on WiMAX, this work adopts a cybersecurity model could compensate or mitigate the possible threats and does not break the requirements of real time applications of smart grid. It depends on the mutual authentication and robust ciphering technique.

The organization of this research is divided into three sections. Section one explains the introduction and the contributions while section two states the methodology and materials of the suggested network. Section three presents the conclusions.

2. Research Methodology

The current work is an extension to support the designed WCN for the smart grid applications in [16] and [17] by a cybersecurity model in order to prevent or mitigate the possible cyberattacks, where the complete model and the results of system performance are explained in the mentioned works. However, the following subsection handles the assumptions and the description of the adopted model of smart grid.

2.1. The Model Description and The Suggested WCN Infrastructure

The adopted smart grid model consists of one microgrid, 16 electrical substations, advanced metering infrastructure (AMI) and the control center. Hence, the model deals with real time (RT) and non-real time (NRT) applications. In term of RT applications, each electrical substation compromises two industrial clients, wide area control and monitoring (WACM) application that represents phase measuring unit (PMU) [18] [19] and video surveillance [20]. Another real time application is distributed energy resources (DER) where the microgrid sends sampled values to the control center to mirror the status of the microgrid [21] [22].

Table 1. RT applications data description

RT Applications	Data description		
	Data size (byte)	Frequency rate in one second	Data size in one second (KB)
PMU	44	60	2.64
Video surveillance	1024	200	204.8
Microgrid status	256	480	122.8

With respect to NRT applications, smart meters (SMs) of AMI deal with four applications types of non-real time applications: metering, tariffs, alarm, and demand side management (DSM) [23], Table 2 explains the data size of NRT applications.

Henceforth, each 100 SMs are connected to one SM concentrator to handle the data of AMI from/to SMs to/from AMI servers. The whole data of the model are exchange between the applications of nominal structures and the control center via the designed WCN infrastructure of smart grid. The WCN infrastructure (base stations) of smart grid based on WiMAX system is self-powered and it depends on renewable energy system, solar power, and storage system instead of the conventional power grid, as shown in [16] and [17]. In addition, the WCN is enhanced by edge computing based on wireless fashion to support the control center processing in terms of servers' reliability, compensate heavy data, and smaller latency compared to the case without edge computing. It is worth to mention, the model of smart grid WCN is built using OPNET Modeler.

This research addresses the proposed infrastructure for smart grid applications in three different scenarios.

Scenario_1: WiMAX BSs cover the proposed wide area network of the smart grid; all clients of smart grid connect wirelessly to BSs. The utility of the smart grid owns the servers based on WiMAX technology.

Scenario_2: This scenario is similar to the first scenario but: (1) WiMAX BSs are connected to the control center using point to point protocol (PPP) digital signal level 3 (DS3) cable (2) the processing of collected data at the control center is implemented using servers based-Ethernet under the property of the utility of smart grid.

Scenario_3: This scenario is similar to the scenario one with employing the edge computing using local servers based-WiMAX, the servers are placed near to clients to take the advantage of fast processing and addressing the availability and the reliability. In this case, clients deal with local severs of the edge computing locally and there are connections between the local servers and the main servers at the control center of smart grid in order to receive any update or sending a copy of the data. However, the main assumptions of WiMAX are shown in Table 3. Table 4 states the suggested self-powered WCN infrastructure based on

WiMAX [24] [25] [26] [27]. It is worth to mention that, the details of self-powered WCN design are explained in [16].

Table 2. AMI applications data description

NRT Applications	Advanced metering infrastructure (AMI)		Data size (byte)	Frequency rate
	Source	Destination		
AMR	AMI Server	SM	101	15 min
	SM	AMI Server	89	
System alarm	AMI Server	SM	21	Based indicator events (it is assumed 15 min)
	SM	AMI Server	115	
Tariffs	AMI Server	SM	445	15 min
	SM	AMI Server	13	
DSM	AMI Server	SM	53	Based indicator events (it is assumed 15 min)
	SM	AMI Server	67	

Table 3. WiMAX assumptions of suggested WCN

Assumption	Description
Bandwidth	20MHz
Modulation scheme	16QAM
Coding rate of DL/UL	¾ / ½
No. of sector/BS	3
Duplexing mode	Time Division Duplexing (TDD)
Symbol length	102.86µ sec
Frame length	5 m sec
QoS	RTPS (for RT applications) and NRTPS (for AMI applications)

Table 4. WiMAX assumptions of suggested WCN

2.2. *Threats Model of The Suggested WCN based on WiMAX*

Although the WiMAX system appears to be secured due to the integration of security functionalities in the sublayer of security partitioning in the MAC layer, several security vulnerabilities are indicated and described in the literature.

Case	Load (w)	Self-powered WCN based on solar system		
		Batteries		No. of solar panels
		No. of (200 AH)	Delivered electricity continuously (hours) until full discharging	Capacity 660w
BS sector without cooling system	**1064**	**2**	**18**	**3**
BS sector with cooling system	**1754**	**3**	**16**	**5**
Server	**150**	**1**	**64**	**1**
BS sector and server with cooling system	**1904**	**3**	**15**	**6**
Three BS sectors and server with cooling system	**3872**	**6**	**15**	**11**

Most of them are relevant to authentication, key management, and availability [28] [29].

In the phase of authorization, the client could authenticate itself to the BS by sending its certificate. However, the BS does not authenticate itself to the client. In this case, an attacker could claim to be a legitimate BS in order to implement a rogue BS attack. As a result, the attracted client may be tried to attach itself to the rouge BS (attacker). The attacker handles the identity of BS and he waits until starting the time slot that allocated to the origin BS. Additionally, the attacker may transmit the message with high signal magnitude to force the targeted client to drop the signal of the legitimate BS. At this level, the client starts the authorization phase with the fake BS by sending two messages of request the authorization (authorization information message and authorization request message). When the rouge BS receives these messages, it sends the response (authorization response message) to the targeted client. The message of the authorization response includes AK that is encrypted by the client's public key. The targeted client receives the nominal message but he cannot verify the authenticity of this message, therefore he derives the key and HMAC of uplink and downlink from the received AK. Consequently, the attacker gains control over the communication of client and he could register himself at the legitimate BS by the credentials of targeted clients (MITM attack).

On the other hand, the phase of key management is also vulnerable to the replay attack. Hence, the client in some situations cannot recognize between a new data SA and reused data SA because the key response message (PKM-RSP) does not own sufficient information about the sender's authenticity. However, each client holds two keying materials (old TEK and new TEK). When the client requests the materials of keying for the first time, the attacker could execute a replay attack. Another case, the attacker could capture the messages of key request and key response, then

he waits the second phase when privacy key management is reset. In such case, the client will request new keying materials, henceforth the attacker could replay the copy of key response message.

In the context of availability, the attacker could exploit the authorization request message that does not include any field explaining the validity (freshness) of the messages. As a result, the system becomes vulnerable to the replay attack, where the attack intercepts the nominal message and stores it. Later, the attacker could send the message repeatedly to the BS (DoS attack).

As explained previously, WiMAX system suffers from some threats regarding the phase of connection initialization and establishment. The works in [30] [31] [32] [33] [34] [35] and [36] highlighted the main vulnerabilities of WiMAX system that are related to unauthenticated management messages, unencrypted management MAC messages, and shared keys in multicast and broadcast, Table 5 illustrates the vulnerabilities of the suggested WCN based on WiMAX system, possible attacks, and the suggested solutions.

Table 5. Possible attacks on the suggested WCN

WCN-based WiMAX vulnerabilities	Explanation	Possible attacks
Unauthenticated management messages	Broadcast messages are difficult to protect since there is no common key (an adversary listens to the traffic)	Forged messages
Unencrypted management MAC messages	Management MAC messages are never encrypted (an adversary listens to the traffic)	Eavesdropping, MITM, DoS
Interleaving attack	Attacker impersonates a legal client; he sends an authorization information message based on intercepted sessions. Then, he received the response from BS. To send an ack, he should own the key to encrypt the message so he claims to be BS to target another client using the information of authorization response. He receives authorization acknowledgement message from nominal client. Later, he completes the pending uncompleted session with the BS.	MITM, Reply
Authorization vulnerabilities	If a response authentication message is lost from BS to a client, then the client resends the request. BS will resend the response (because BS could not compute if this reply attack or not where no feedback from the client). In this case, an intruder can flood the BS with authentication request messages	Reply, DoS
RF jamming	Introducing a powerful RF source intended to overwhelm system radio spectrum	DoS

2.3. *The Adopted Security Model*

The suggested WCN serves different applications in terms of RT and NRT applications. It is assumed that, each application under the specific facility is protected as shown in the electrical substation. However, this subsection discusses how to secure the data flow of WCN based on WiMAX system, see Figure 1

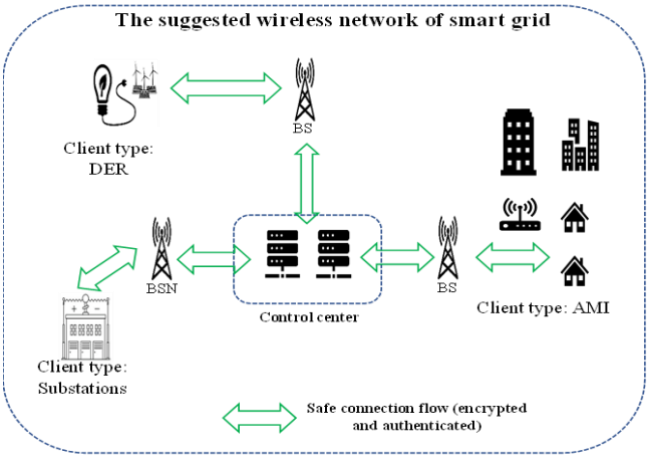

Fig. 1. The connections flow of the suggested WCN.

In the adopted model of security, the client represents phasor measurements of the substation (wide area monitoring applications), microgrid monitoring application (distributed energy resources application), or smart meter concentrator (advanced measurement infrastructure applications). Before transferring secured data in the WiMAX network, each client negotiates with the corresponded BS to acquire the security parameters. Figure 2 shows the privacy key management (PKM) protocol between each client and the corresponded BS [37]. The adopted security model provides encrypted messages to organize the process of network initialization using public and private keys. Further, the security model of the system offers mutual authentication based on the certifications of clients and BS as well as random number (Nonce) as a challenge with respect to the client and the BS.

In the phase of initialization, client firstly initiates the authorization procedures by sending its manufacturing certification to BS (client certification). In this phase, there is no response from BS, but the corresponded BS compares between the receiving certification from the client during this phase and the received certification. of the client in the following phase (authorization request) to ensure the authentication of the sender [37] [38].

The following phase is the authentication key (AK) authorization that includes three messages (request, reply, and confirm). The authorization request message is sent from the client to BS. This message consists of client certification, the random number from the client; Nonce (Nc), the cryptographic capability descriptions that supported by the client, and SA identifiers (SAID). The previous message is encrypted by the client signature (signed by the private key of the client). The BS receives the request message and it checks the certification of the client (with the received cert. in the initialization phase). Then, the BS decrypts the signature of the client to verify the validity of the message (for authentication purposes). If the request message is valid, BS activates a Pairwise Master Key (PMK) that derives an AK and the public key of the SS by analyzing capabilities.

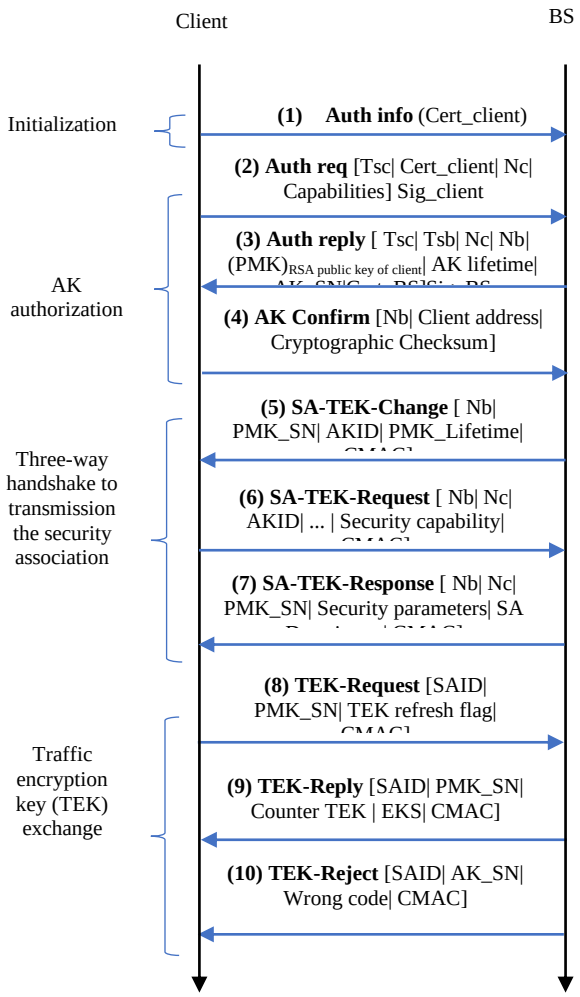

Fig. 2 The security negotiations between a client and BS of the suggested WCN.

It is worth to mention, to protect the BS from replay attacks on the authorization request message, a list of previously received nonces by the same client should be listed in order to detect replayed messages. Further, it is possible to add a timestamp in the request and replay messages to prevent against replay attack instead of Nonce. In such case, it has added a timestamp that is generated by the client (Tsc) in the request message of authorization. While in the BS side, it is added a copy of the client timestamp in addition to generate a timestamp at BS (Tsb) in the response message of the authorization. When the client receives the response message of authorization, it checks a threshold value based on the difference between the timestamp of Tsc and Tsb to prevent the replay attack [28]. In fact, the Nonces exchanging only ensures client that the message authentication replay is a reply corresponding to its request. However, the BS still faces the reply attack because BS cannot tell whether the message of authentication request is recent message or an old message [39].

Then, the BS sends the response message authentication including AK that is encrypted by the public key the client, Nonce of the client, Nonce of BS (Nb), and BS's certification (BS Cert.) [40]. The message of authentication response is encrypted by BS. At the last of this phase, the client sends a confirmation message to the BS. The three-way handshake of the security association transmission starts after addressing the authorization phase. All messages of this phase are encrypted by the ciphering message authentication code; CMAC (a public key known by both client and BS) [41]. The last phase of privacy key management is the TEK exchange (the key that is used for encrypting the exchanged data between the client and the BS). This phase consists of two messages either TEK request with TEK reply, or TEK request with TEK reject. The request message of TEK contains SAID. If the SAID is no longer valid, a TEK-Reject message is sent by BS to inform that the client hasn't applied for a TEK successfully. Else, the reply will be positive. The encryption key is derived from AK.

2.4. *System Performance Results and Discussions*

Firstly, this part discusses the effect of the ciphering algorithm on the most time-sensitive RT application (i.e, PMU application) in the suggested model in order to explain the effect of encryption algorithm on the latency requirement of the RT applications. Hence, it is essential to explain that the suggested ciphering algorithm should never break the requirements of application in term of the latency.

In the adopted cybersecurity model of WCN based on WiMAX infrastructure, the algorithm of encryption is AES_128 as mentioned previously. Figure 3 explains the effect of WCN encryption on the application of PMUs (16 clients) in the case of processing rate of each PMU client is 5000 packets/sec and the reserved traffic per connection in WiMAX is 50kbps.

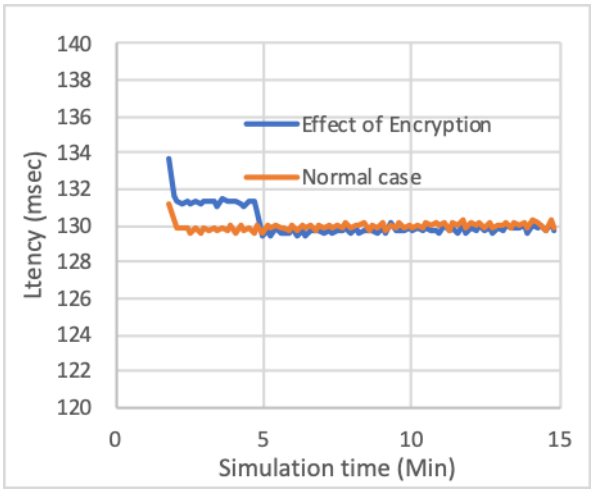

Fig. 3 Effect of encryption on PMU application latency in case of reserved traffic is 50kbps and processing rate is 5000 packet/sec.

The Figure declares two cases in term of latency where the first case is "Normal case" that represents the latency in the case of no encryption in WCN while the second case is the latency of the PMU application with the case of AES-128 encryption. It is noted that, the effect of encryption is a slight and the latency is about 130 msec in the two cases after the fifth minute of the simulation time.

Figure 4 demonstrates the effect of encryption on the system in the case of upgrading the processing rate of the

field device (the processing rate per PMU client is 10000 packet/sec). Whilst, Figure 5 explains the effect of encryption in the case of increasing the reserved traffic per connection to 384kbps and the processing rate per PMU client is 10000 packet/sec. It is obvious that, the effect of encryption on the latency of the system is very little. Hence, the latency of the system with the encryption in Figure 4 is less than 25msec. Consequently, the encryption algorithm in the WCN based on WiMAX does not break the requirement of real time application latency.

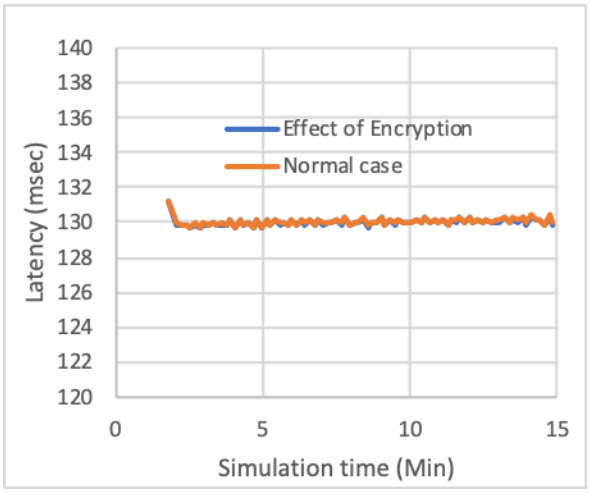

Fig. 4 Effect of encryption on PMU application latency in case of processing rate per client is 10000 packet/sec.

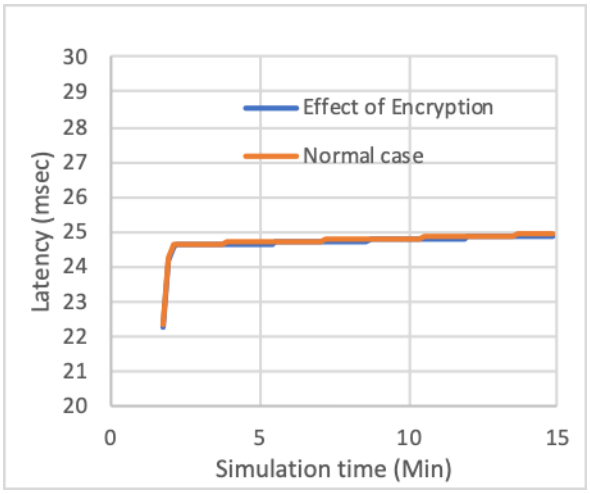

Fig. 5 Effect of encryption on PMU application latency in case of reserved traffic is 384 kbps and processing rate per client is 10000 packet/sec.

Figure 6 shows the global latency in terms of Minimum, Average, and Maximum values with respect to 16 video surveillances clients for all adopted scenarios: scenario_1, scenario_2 and scenario_3. The maximum latency of the first scenario is about 642 msec because the BS sector cannot handle the required capacity of video surveillance for 16 substations.

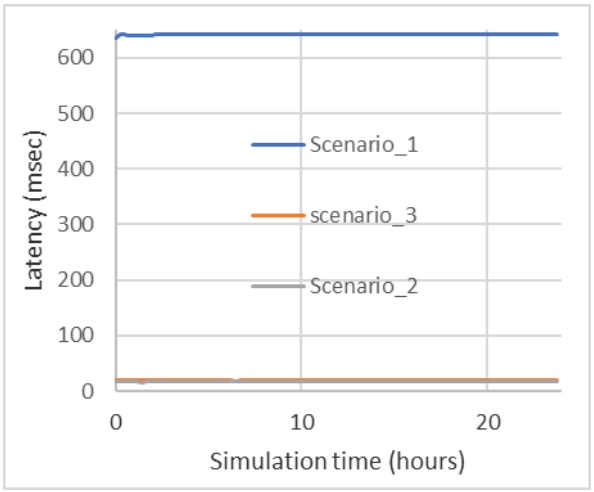

Fig. 6 Latency of 16 video surveillance clients with different scenarios.

The results indicate that the employing of edge computing (scenario_3) improves the latency of the system significantly compared to scenario_1. Consequently, scenario_3 handles a perfect magnitude of latency as well as the features of flexibility and low-cost maintenance compared to the pure wireless system and the scenario of cabling backbone of the smart grid. In other words, scenario_3 submits the advantages of scenario_1 and scenario_2. According to the requirements of video surveillance application, the threshold of the video latency should be less than 200 msec [6].

Table 6 presents all applications of the adopted smart grid together in one view. This Table handles three different cases to distribute the real time applications of smart grid on the capacity of one BS (three sectors). Case one explains that the capacity of one BS sector can compensate 6 clients of video without impairments where all sent traffic is received successfully with a small latency. However, the adopted typical smart grid has 16 clients of video surveillance. Case two shows that, adding any extra clients to Sector one or Sector two of BS could raise the latency hugely and causing packet loss. While case three demonstrates the suitable adding of the rest of the video clients (4 clients of video surveillance) should link to the Sector three because the traffic of other applications (DER and PMUs) is relatively small compared to video surveillance application. In summary, case three is the efficient distribution to the clients of RT applications to handle the optimum latency and traffic of the wireless scenario in the adopted typical smart grid.

The adopted applications of non-real time are Alarm, AMR, Tariffs, and DSM (AMI applications), these applications deal with transmission control protocol (TCP) protocol to provide the reliability. The vital metric of non-real time applications is the received data reliability to prove that all sent traffic is received successfully while the latency does not consider the more significant metric for non-real time applications. Table 7 explains the traffic in terms of sent and received data of AMI applications in scenario_1 with 30000 SMs. All sent data is received correctly (i.e., the reliability of received data is 100%). It is worth to mention

that, the frequency rate of AMI applications is each 15 minutes.

Table 6. Real Time Applications Together

case	ONE BS (Load of the BS sectors)			Traffic (M byte/sec)		Max Global Latency (msec)
	Sector1	Sector2	Sector3	Sent	Received	
1	6 video clients	6 video clients	16 PMUs clients and one Microgrid	**2.627**	**2.627**	**19.5**
2	7 video clients	6 video clients	16 PMUs clients and one Microgrid	**2.832**	**2.642**	**127.9**
3	6 video clients	6 video clients	16 PMUs clients, one Microgrid, and 4 video clients	**3.447**	**3.447**	**19.88**

Table 7. NRT Traffic for AMI applications in the Case of 30000 SMs

Alarm: Traffic (Byte/sec) Scenario_1	
Sent	Received
6303	6303
AMR: Traffic (Byte/sec) Scenario_1	
Sent	Received
7809	7809
DSM: Traffic (Byte/sec) Scenario_1	
Sent	Received
5857	5857
Tariffs: Traffic (Byte/sec) Scenario_1	
Sent	Received
15283	15283

The results indicate that the AMI applications do not represent as heavy applications from the size of the data point of view, but the increment in the number of smart meters may lead to forming a burden on the capacity of WiMAX BS sector and the servers in the control center.

Figure 7 shows the effect of proposed infrastructure scenarios on the packet network delay of Tariffs application at 30000 SMs (maximum adopted number of SMs per BS) to explain the performance of the designed infrastructure. Case_2 (scenario_2) and case_3 (scenario_3) offer smaller delay compared to case_1. It is worth to mention, each 10000 SMs are linked to one BS sector.

All scenarios present an acceptable delay with respect to AMI application [42]. However, the maximum recorded delay is less than 600 msec while the threshold of AMI applications reaches up to 2 seconds.

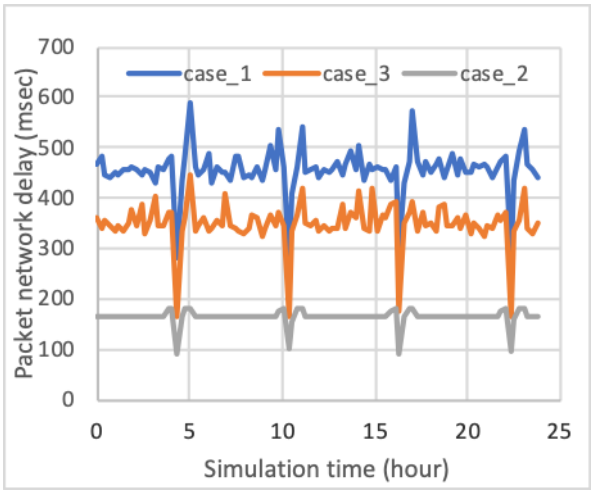

Fig. 7 Packet network delay for 30000 SMs in the case of Tariffs application.

2.5. *Security Analysis of The Suggested WCN*

This subsection highlights the mechanisms of compensate the vulnerabilities of the suggested wireless network based on WiMAX system by the corresponded countermeasures. As shown earlier, the main vulnerabilities of the WiMAX infrastructure are related to protecting the initialization phases that suffer from absent the appropriate encryption and authentication methods, while the phase of data transfer in a WiMAX system owns robust countermeasures in terms of encryption, authentication, and data integrity. The current work focuses on enhancing the security countermeasures in the initialization phase between the client and the BS suggestion the mutual authentication and asymmetric encryption. Table 8 demonstrates the suitable countermeasures against the possible attacks.

Table 8. The Countermeasures Against the Possible Attacks in WiMAX System

WiMAX vulnerabilities	Suggested solutions
Unauthenticated management messages	Mutual authentication and adding BS cert. Using CMAC or Short HMAC to add integrity. In addition, addressing symmetric encryption outside the sharing group may increase the security, or an asymmetric key are exploited. The private key of the BS is used to sign the management messages. The client verifies the received messages by public key
Unencrypted management MAC messages	An agreed encryption mechanism among the authenticated parties such as (Diffie-Hellman key)
Interleaving attack	Using CMAC or Short HMAC with key
Authorization vulnerabilities	Mutual authentication and Integrity check: digest to ensure the message was not modified (Using CMAC or Short HMAC)
RF jamming	Locate and remove the source of RF interference or to move to another channel

Finally, Table 9 submits a comparison between this work during the term of the wireless network of smart grid and the previous works.

Table 9. Comparison Among This Work and Previous Related Works

Work	RT	NRT	Self-powered system and green communication	BS capacity analysis	Decentrali-zed computing (Edge)	Cyber security model	Method	Metric
[43]	Y	N	N	N	N	N	Qualnet	Delay, Throughput, Packet delivery
[44]	Y	Y	N	N	N	N	OPNET	Delay
[45]	Y	N	N	Y	N	N	OPNET	Error rate, Throughput, capacity, Latency
[46]	N	Y	N	N	N	N	OPNET	Signal to noise ratio, Delay, packet drop
[10]	Y	Y	N	N	N	N	OPNET	Capacity, packet loss, latency, throughput
This work	Y	Y	Y	Y	Y	Y	OPNET , analysis	Latency, traffic sent, traffic received, capacity, capacity, packet losspower consumption

3. Conclusion

This research proposes secured self-powered wireless communication infrastructure based on WiMAX system for the smart grid applications.

The results indicate the employing of wireless edge computing reduces the latency of video surveillance application about 34 times with more than 99.99% data reliability compared to the wireless scenario without employing the edge computing. Whilst, DER data is a very time sensitive application required hard conditions. The adopted wireless scenario can address these requirements in the case of dealing with one Microgrid at reserved data rates equal to 0.5M bps where the latency is less than 19 msec and the lost packet is null.

The suggested wireless network infrastructure can handle the requirements of AMI applications for all scenarios, because this type of applications is not sensitive to the time. The increment of SMs in AMI infrastructure forms a heavy burden on the servers of the control center. Employing the edge computing improves the performance of the WCN from packet network delay and the reliability.

During the term of cybersecurity, the WiMAX system is built based on a robust security model compared to the WLAN standards. But this model suffers from some issues in the authentication phases. This research presents an enhancement to the initial security model of WiMAX to improve the security model of the suggested smart grid WCN. Mutual authentication in the phase of the authentication in addition to add Nonce and time stamp contribute in enhancing the model of authentication to protect the clients of the field in the smart grid. On the other hand, the ciphering algorithm in WiMAX should never break the requirements of real time applications in term of latency. Therefore, the AES-128 algorithm can offer suitable protection against adversary in the case of handling the robust level of cybersecurity in the phases of authentication and key exchanges.

Acknowledgements

The authors are very grateful to the University of Mosul / College of Engineering for their provided facilities, which helped to improve the quality of this work.

References

[1] M. Deruyck, W. Vereecken, E. Tanghe, W. Joseph, M. Pickavet, L. Martens, P. Demeester, “Power consumption in wireless access network,” in 2010 European Wireless Conference (EW), Apr. 2010, pp. 924–931. doi: 10.1109/EW.2010.5483506.

[2] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, “Cybersecurity for distributed energy resources and smart inverters,” IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 28–39, 2016, doi: 10.1049/iet-cps.2016.0018.

[3] J.-L. Batard, Y. Chollot, P. Pipet, L. Lamberti, and A. Gauci, “Cybersecurity for modern distribution automation grids,” CIRED - Open Access Proceedings Journal, vol. 2017, no. 1, pp. 1002–1005, Oct. 2017, doi: 10.1049/oap-cired.2017.1328.

[4] S. Xu, Y. Qian, and R. Q. Hu, “Reliable and resilient access network design for advanced metering infrastructures in smart grid,” IET Smart Grid, vol. 1, no. 1, pp. 24–30, Apr. 2018, doi: 10.1049/iet-stg.2018.0008.

[5] M. Zeinali and J. Thompson, “Comprehensive practical evaluation of wired and wireless internet base smart grid communication,” IET Smart Grid, vol. 4, no. 5, pp. 522–535, Mar. 2021, doi: 10.1049/stg2.12023.

[6] M. Islam, M. M. Uddin, M. A. A. Mamun, and M. A. Kader, "Performance analysis of AMI distributed area network using WiMAX technology," in 2014 9th International Forum on Strategic Technology (IFOST), Oct. 2014, pp. 152–155. doi: 10.1109/IFOST.2014.6991093.

[7] P. P. S. Priya and V. Saminadan, "Performance analysis of WiMAX based Smart grid communication traffic priority model," in 2014 International Conference on Communication and Signal Processing, Apr. 2014, pp. 778–782. doi: 10.1109/ICCSP.2014.6949949.

[8] G. D. Castellanos and J. Y. Khan, "Performance analysis of WiMAX polling service for smart grid meter reading applications," in 2012 IEEE Colombian Communications Conference (COLCOM), May 2012, pp. 1–6. doi: 10.1109/ColComCon.2012.6233661.

[9] B. Al-Omar, T. Landolsi, and A. Al-Ali, "Evaluation of WiMAX Technology in Smart Grid Communications," J. Commun., 2015, doi: 10.12720/jcm.10.10.804-811.

[10] O. Neagu and W. Hamouda, "Performance of WiMAX for smart grid applications," in 2016 International Conference on Selected Topics in Mobile Wireless Networking (MoWNeT), Apr. 2016, pp. 1–5. doi: 10.1109/MoWNet.2016.7496613.

[11] H. Khan, Reduan, and Y. Khan. Jamil "Wide area PMU communication over a WiMAX network in the smart grid." 2012 IEEE third international conference on smart grid communications (SmartGridComm). IEEE, 2012.

[12] J. Akram, A. Tahir, H. S. Munawar, A. Akram, A. Z. Kouzani, and M. A. P. Mahmud, "Cloud- and Fog-Integrated Smart Grid Model for Efficient Resource Utilisation," Sensors, vol. 21, no. 23, Art. no. 23, Jan. 2021, doi: 10.3390/s21237846.

[13] N. Mishra, V. Kumar, and G. Bhardwaj, "Role of Cloud Computing in Smart Grid," in 2019 International Conference on Automation, Computational and Technology Management (ICACTM), Apr. 2019, pp. 252–255. doi: 10.1109/ICACTM.2019.8776750.

[14] M. Talaat, A. S. Alsayyari, A. Alblawi, and A. Y. Hatata, "Hybrid-cloud-based data processing for power system monitoring in smart grids," Sustainable Cities and Society, vol. 55, p. 102049, Apr. 2020, doi: 10.1016/j.scs.2020.102049.

[15] M. Forcan and M. Maksimović, "Cloud-Fog-based approach for Smart Grid monitoring," Simulation Modelling Practice and Theory, vol. 101, p. 101988, May 2020, doi: 10.1016/j.simpat.2019.101988.

[16] F. Alsharbaty and Q. Ali, "Self-Powered Wide Area Infrastructure Based on WiMAX for Real Time Applications of Smart Grid," Iraqi Journal for Electrical and Electronic Engineering, vol. 18, pp. 92–100, Dec. 2022, doi: 10.37917/ijeee.18.2.12.

[17] F. S. Alsharbaty and Q. I. Ali, "RESILIENCE AND SELF-POWERED WIMAX SYSTEM ENHANCED BY FOG COMPUTING FOR SMART GRID APPLICATIONS," Quantum Journal of Engineering, Science and Technology, vol. 3, no. 2, Art. no. 2, Jul. 2022.

[18] "IEEE Standard for Synchrophasor Data Transfer for Power Systems," IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005), pp. 1–53, Dec. 2011, doi: 10.1109/IEEESTD.2011.6111222.

[19] Obaidat, M., Anpalagan, A., & Woungang, I. (Eds.). (2012). Handbook of green information and communication systems. Academic press.

[20] D. Babazadeh, M. Chenine, K. Zhu, L. Nordström, and A. Al-Hammouri, "A platform for wide area monitoring and control system ICT analysis and development," presented at the 2013 IEEE Grenoble Conference, 2013, pp. 1–7.

[21] P. Parikh, "Investigation of Wireless LAN for IEC 61850 based Smart Distribution Substations," Electronic Thesis and Dissertation Repository, Aug. 2012, [Online]. Available: https://ir.lib.uwo.ca/etd/869

[22] A. C. Z. de Souza and M. Castilla, Microgrids design and implementation. Springer, 2019.

[23] Y. He, "Smart metering infrastructure for distribution network operation," Diss. Cardiff University, 2016.

[24] M. H. Alsharif, "Comparative Analysis of Solar-Powered Base Stations for Green Mobile Networks," Energies, vol. 10, no. 8, Art. no. 8, Aug. 2017, doi: 10.3390/en10081208.

[25] M. Deruyck et al., "Power consumption in wireless access network," in 2010 European Wireless Conference (EW), Apr. 2010, pp. 924–931. doi: 10.1109/EW.2010.5483506.

[26] F. E. Office, "Mobile WiMAX Base Station Architecture and RF Technology," FUJITSU Sci. Tech. J., p. 8, 2008.

[27] "A Solar-Powered WiMAX Base Station Solution," studylib.net. https://studylib.net/doc/18419484/a-solar-powered-wimax-base-station-solution (accessed May 13, 2022).

[28] Muller, P., Sharif, H., & Tang, S. Y. (Eds.). (2011). WiMAX security and quality of service: an end-to-end perspective. John Wiley & Sons.

[29] K. Scarfone, C. Tibbs, and M. Sexton, Guide to Securing WiMAX Wireless Communications: Recommendations of the National Institute of Standards and Technology. CreateSpace Independent Publishing Platform, 2012.

[30] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, "Security advances and challenges in 4G wireless networks," in 2010 Eighth International Conference on Privacy, Security and Trust, Aug. 2010, pp. 62–71. doi: 10.1109/PST.2010.5593244.

[31] C. Kolias, G. Kambourakis, and S. Gritzalis, "Attacks and Countermeasures on 802.16: Analysis and Assessment," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 487–514, 2013, doi: 10.1109/SURV.2012.021312.00138.

[32] M. S. Rahman and M. Md. S. Kowsar, "WiMAX security analysis and enhancement," in 2009 12th International Conference on Computers and Information Technology, Dec. 2009, pp. 679–684. doi: 10.1109/ICCIT.2009.5407321.

[33] A. Sanjay P. and C. Nicole, "An Assessment of WiMax Security," Communications and Network, vol. 2010, May 2010, doi: 10.4236/cn.2010.22020.

[34] P. Schoinas, "Secure military communications on 3G, 4G and WiMAX," Thesis, Monterey, California: Naval Postgraduate School, 2013. Accessed: Aug. 09, 2022. [Online]. Available: https://calhoun.nps.edu/handle/10945/37712

[35] K. Scarfone, C. Tibbs, and M. Sexton, "Guide to Securing WiMAX Wireless Communications," National Institute of Standards and Technology, NIST Special Publication (SP) 800-127 (Withdrawn), Sep. 2010. doi: 10.6028/NIST.SP.800-127.

[36] S. Woo and G. Jeong, "A Study of WiMAX Security threats and Their Solution," International Journal of Internet, Broadcasting and Communication, vol. 8, no. 2, pp. 66–74, 2016, doi: 10.7236/IJIBC.2016.8.2.66.

[37] J. Jiang, H. Mao, R. Shao, and Y. Xu, "Formal Verification and Improvement of the PKMv3 Protocol Using CSP," in 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Jul. 2018, vol. 02, pp. 682–687. doi: 10.1109/COMPSAC.2018.10318.

[38] S. Xu, S. Yang, and K. Zhang, "Formal Analysis of SA-TEK 3-Way Handshake Protocols," J. Shanghai Jiaotong Univ. (Sci.), Aug. 2021, doi: 10.1007/s12204-021-2340-2.

[39] M. R. K. Siddiqui and S. M. A. Rahman, Security analysis of the WiMAX technology in Wireless Mesh networks. 2009. Accessed: Nov. 11, 2022. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:bth-3039

[40] P. K. Panda and S. Chattopadhyay, "A modified PKM environment for the security enhancement of IEEE 802.16e," Computer Standards & Interfaces, vol. 61, pp. 107–120, Jan. 2019, doi: 10.1016/j.csi.2018.06.002.

[41] A. Braeken, "Public key versus symmetric key cryptography in client–server authentication protocols," Int. J. Inf. Secur., vol. 21, no. 1, pp. 103–114, Feb. 2022, doi: 10.1007/s10207-021-00543-w.

[42] R. Siqueira de Carvalho, P. Kumar Sen, Y. Nag Velaga, L. Feksa Ramos, and L. Neves Canha, "Communication System Design for an Advanced Metering Infrastructure," Sensors, vol. 18, no. 11, Art. no. 11, Nov. 2018, doi: 10.3390/s18113734.

[43] F. Gómez-Cuba, R. Asorey-Cacheda, and F. J. González-Castaño, "WiMAX for smart grid last-mile communications: TOS traffic mapping and performance assessment," in 2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Oct. 2012, pp. 1–8. doi: 10.1109/ISGTEurope.2012.6465616.

[44] Al-Omar, Ban, Taha Landolsi, and Abdul-Rahman Al-Ali. "Evaluation of WiMAX Technology in Smart Grid Communications." J. Commun. 10.10 (2015): 804-811.

[45] O. Neagu, "WiMAX for Smart Grid Applications and the Influence of Impulsive Noise," masters, Concordia University, 2015. Accessed: May 01, 2022. [Online]. Available: https://spectrum.library.concordia.ca/id/eprint/980660/

[46] S. Premkumar, Dr. V. Saminadan, and Pondicherry Engineering College, "Performance Analysis of WLAN-WiMAX Smart Distribution Grid," IJERT, vol. V4, no. 08, p. IJERTV4IS080595, Aug. 2015, doi: 10.17577/IJERTV4IS080595.