Mona Almansoori[1,*], Ahmad Elshamy[2], and Ahmad Mustafa[2]

[1] Suez Canal University, Department of Mathematical, Faculty of Science, Computer Science unit, 43711 Suez, Ismailia, Egypt
[2] British University, Computer Science Department, 11837 Cairo, Egypt.

* Corresponding author: mnmalmansoori@gmail.com; Tel.: +971-505-686-660

Title:

Secure Z-MAC Protocol as a Proposed Solution for Improving Security in WSNs

IECI 2021

Abstract:

Security is one of major issues in WSNs as poor security disrupts the entire network and can have a significant effect on data transmission. So, the focus of the current research is to develop a secure Z-MAC protocol along with the implementation of elliptic curve encryption and IHOP mechanism. Basic Z-MAC protocol and secure Z-MAC protocol were compared in terms of the stages and performance while they were introduced with blackhole, flooding, and DDOS attacks. It was found that secure Z-MAC protocol ensures high security and performance even when the network is introduced with variety of attacks. It was also observed that delay in packets was minimal when secure Z-MAC protocol was implemented in the network.

Keywords: Security in WSNs; security attacks; Z-MAC protocol; secure Z-MAC protocol

Introduction:

- The Z-MAC protocol enables to have minimal contention, fast throughput, shorter latency, lower power consumption, and improved efficiency[1], because of weak data integrity and encryption methods, wireless sensor networks are readily hacked.
- This research focused on increasing the security of WSNs by developing a more secure and safe Z-MAC protocol.

Objectives:

- WSN require efficient secure data transmission using low processing power and maintaining data integrity which is partially provided by Z-MAC
- Proposed a secure data transmission solution modifying the z-mac for secure data transmission using IHOP and Eliptic curve.
- Encrypt packets using the Eliptic curve for efficient and lightweight properties
- Prove that it can achieve a high throughput without being compromised

1. Rhee, I., Warrier, A., Aia, M., Min, J., & Sichitiu, M. L. Z-MAC: a hybrid MAC for wireless sensor networks. IEEE/ACM Transactions On Networking 2008, 16(3), 511-524. 10.1109/TNET.2007.900704

Literature Review:

- **Problem Statement**
  - Numerous attacks, such as DDOS attacks, flooding attacks, and blackhole attacks, can arise in a WSN, compromising the network's security and efficiency.
  - To guard against such attacks in a WSN, there is a protocol known as the Z-MAC protocol that utilizes TDMA and CSMA mechanisms. This Z-MAC protocol has inherent limitations that compromise the network's security, including cost constraints related with slot assignment and clock synchronization, excessive energy consumption, synchronization issues, and concealed terminal issues [2].
- **Suggested Solution**
  - To overcome the issue of security in the Z-MAC protocol, a secure Z-MAC protocol has been developed.
  - Secure Z-MAC protocol would occur in seven developed stages, such as neighbour discovery and slot assignment, local framing, transmission control, explicit contention notification, receiving schedule of Z-MAC, and local time synchronization, which are a part of IHOP mechanism.

2. Arshad, S., Al-Sadi, A., & Barnawi, A. (2013). Z-MAC: performance evaluation and enhancements. Procedia Computer Science, 21, 485-490.

Literature Review:

➢Types of Security Attacks in Networks.

- ❖ Security networks are highly vulnerable to attacks, which allows the hackers to modify data, steal information, attack confidential of individuals. Because sensor networks are scattered, tracking and regulating the true state of the network's elements is a difficult task [3].
- ❖ Common attacks in a WSN are eavesdropping, sinkhole, Denial of Service, flooding, and blackhole attack .

➢Significance of Security in Sensor Networks.

- ❖ Managing security in sensor networks contributes to the authenticity, secrecy, integrity, privacy, and access to data packets.
- ❖ When additional security elements are introduced into the network, the computations, communications, and administration overhead increases in tandem with the increased security effectiveness [4].

3. Kosachenko, T., Dudkin, D., Konev, A., & Sharamok, A. Threat Model for Trusted Sensory Information Collection and Processing Platform. In International Conference on Futuristic Trends in Networks and Computing Technologies, 2020, (pp. 296-304). Springer, Singapore. 10.1007/978-981-16-1483-5_27
4. Du, X., & Chen, H. H. Security in wireless sensor networks. IEEE Wireless Communications 2008, 15(4), 60-66. 10.1109/MWC.2008.4599222

Literature Review:

➢Elliptic curve Encryption

- ❖ Elliptic Curve Encryption (ECE) is a kind of encryption method that may be used to encode and decode data and message authentication, developing digital signatures, and engage in process of exchanging keys[5].
- ❖ The basic process for understanding how ECE works is discussed as follows:

1. A network's nodes decide on an elliptic curve and a fixed curve point F, which are not a secret in the network.
2. Node A selects a secret random integer Ak and it is a secret key and a curve point $A_P = A_k F$ is calculated and it is considered as a public key.
3. Node B also engages in the similar process as done by Node A.
4. Node A randomly selects an integer B_k and it is considered as a secret key, which is not be shared publicly. After that, it calculates the curve point $B_P = B_k F$ as its public key.
5. Once the secret key is generated, Node A wants to send a message to node B.
6. Node A can simply compute $A_k B_P$ and use the final developed outcome as the secret key for encrypting a conventional symmetric block.
7. After this step, Node B can further calculate the similar value by evaluating BkAP, because $B_k A_P = B_k \cdot (A_k F) = A_k \cdot (B_k F) = A_k B_P$

5. Kang, B., Shao, D., & Wang, J. A fair electronic payment system for digital content using elliptic curve cryptography. J. of Algorithms & Comp. Tech. 2018, 12(1), 13-19. https://doi.org/10.1177/1748301817727123

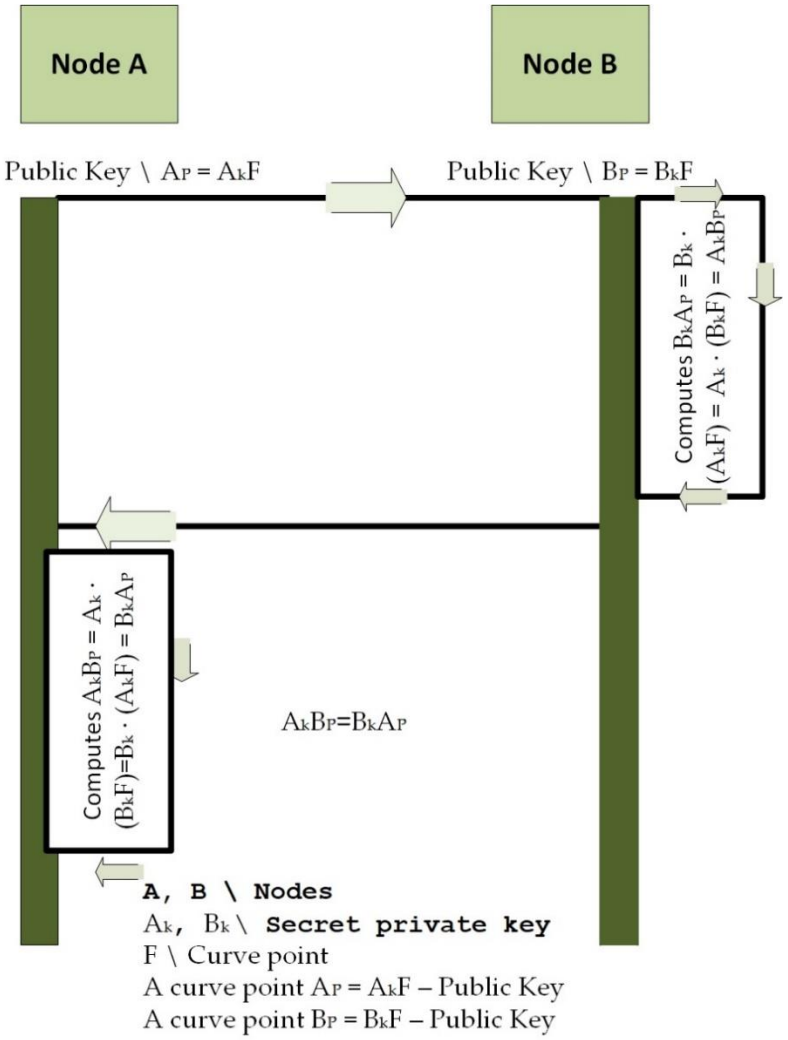
Literature Review:

➢IHOP Mechanism for Key Generation

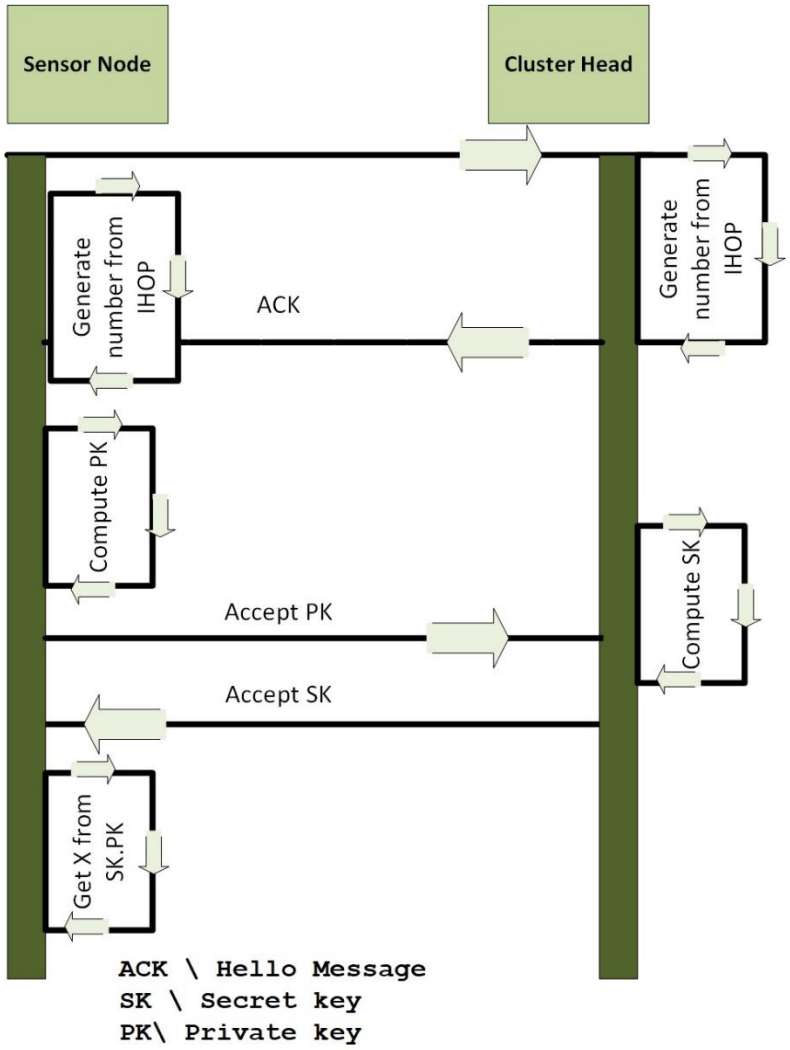
The IHOP mechanism has six stages:

- ❖ Installation and setting up stage for nodes.
- ❖ Association discovery stage, which further has two stages that are known:
  - o Base station hello stage.
  - o Cluster acknowledgement stage.
- ❖ Report endorsement phase, in which t + 1 nodes cooperate to generate a report when they detect the existence of an event occurrence.
- ❖ En-route filtering, involves each sending node to validate the message authentication code (MAC) produced by its subordinate associated and connected nodes before excluding it from the receiving report.
  - o Following successful verification, the node creates and deploys a new MAC with the bilateral key exchanged with the upper connected node. Lastly, it sends the information to its next node throughout the route of the base station.
- ❖ The base station verification stage. If the base station determines that the communication was properly authorized by the t + 1 nodes, it acknowledges

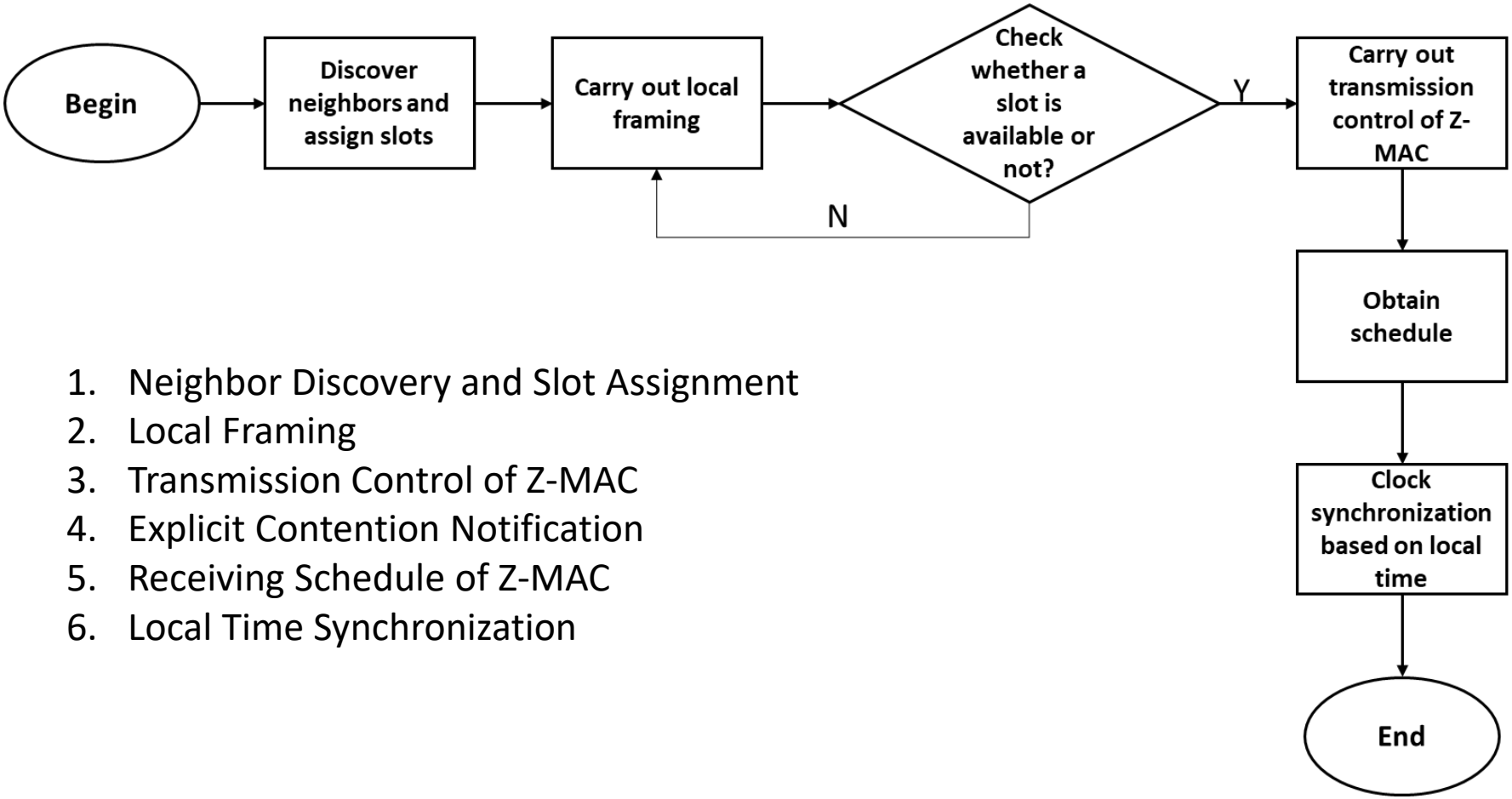
Elliptic Curve Encryption



Key Sharing using IHOP Mechanisms

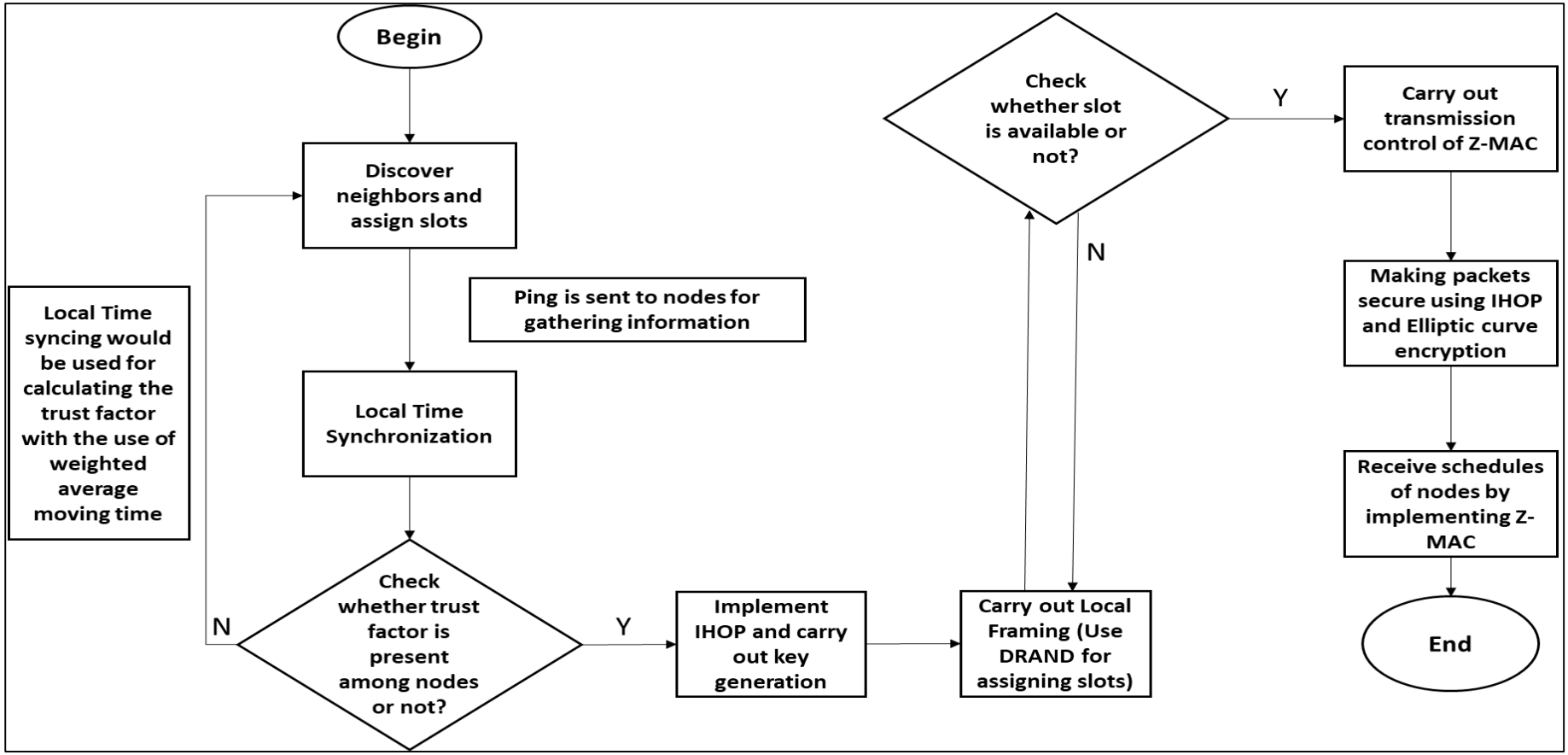


Z-MAC Protocol Operation



1. Neighbor Discovery and Slot Assignment
2. Local Framing
3. Transmission Control of Z-MAC
4. Explicit Contention Notification
5. Receiving Schedule of Z-MAC
6. Local Time Synchronization

Secure Z-MAC Protocol Operation



Secure Z-MAC algorithm

Secure Z-MAC algorithm is presented as follows, which provides a step-by-step understanding of Secure Z-MAC:

Step 1: Begin
Step 2: Conduct neighbor discovery and slot assignment process
Step 3: Send a ping to collect details about the neighboring nodes and to perform local clock synchronization.
Step 4: Check if there is trust factor between the neighboring nodes
    IF ‘Yes’ then Implement IHOP mechanism and generate keys
    IF ‘No’ then repeat Step 2
Step 5: Implement the local framing stage
Step 6: Check if there is a slot available
    IF ‘Yes’ then Carry out Transmission control of Z-MAC protocol
    IF ‘No’ then repeat Step 5
Step 7: Carry out encryption of packets using IHOP mechanism, which is run by ECE
Step 8: Receiving schedule of Z-MAC protocol
Step 9: End

Expermintal setup and Scenarios

The simulations of the current research was done using NS2 simulator.

In all Expermintal implement the following:

- The X-axis indicates the number of packets in bytes.
- The Y-axis represents the transmission time in seconds.
- A network nodes were increased in size by five, repeated until 35-40 nodes.
- The attack vectors were successfully implemented into the nodes, flooding, DDOS, and Black-hole attack.

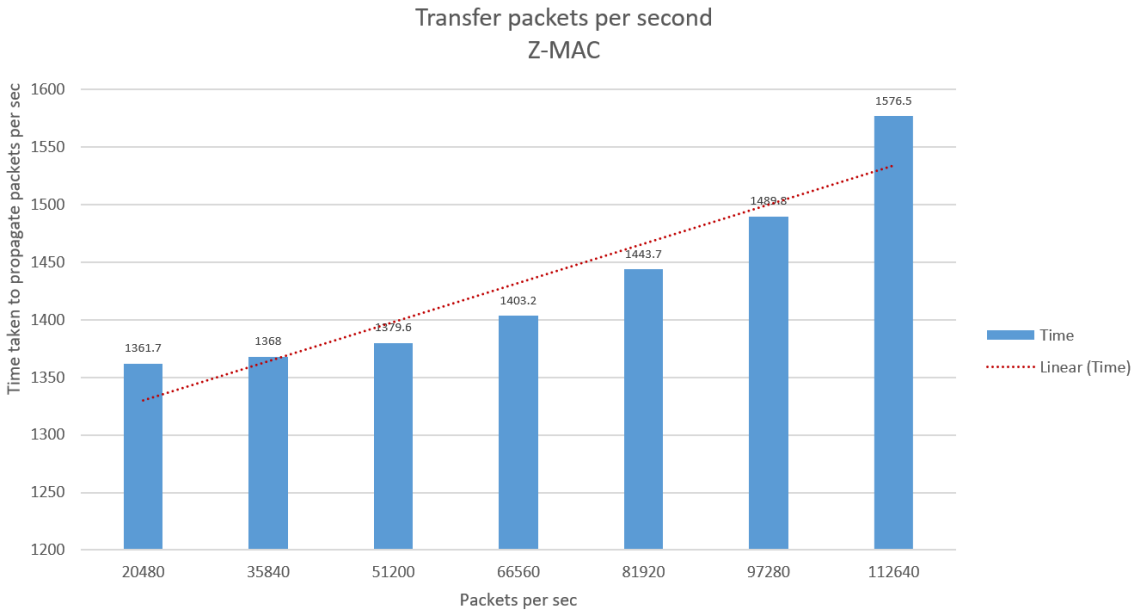
Scenarios as the following :

- Measuring total transmission time using the Z-MAC scheme.
- Measuring number of packets and transmission time during the attack vector introduction against the packets transmitted in Z-MAC scheme.
- Measuring transmission time while implementing IHOP mechanism with Z-MAC protocol.

Experimental Results – Scenario 1

Total transmission time for nodes using the ZMAC scheme

Nodes	Packets/sec in bytes	Time in bits/s
5	20480	1361.78478
10	35840	1367.985821
15	51200	1379.645156
20	66560	1403.241674
25	81920	1443.686908
30	97280	1489.758152
35	112640	1576.497647



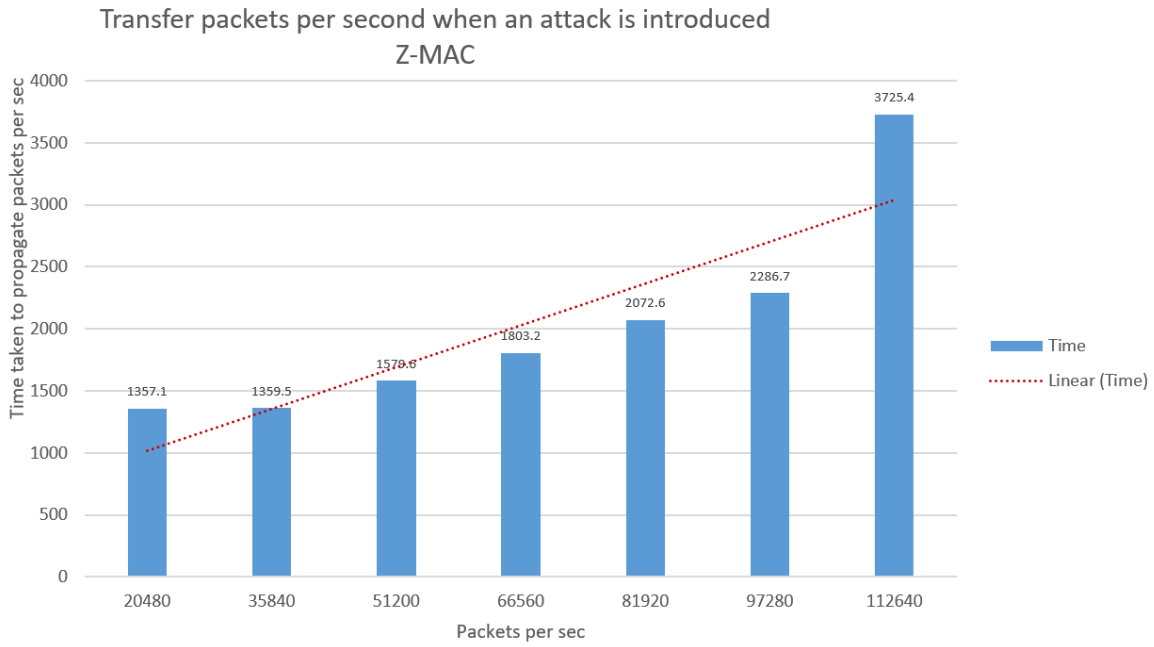
Transmission Time using Basic Z-MAC Protocol

IECI 2021

Experimental Results – Scenario 2

Total transmission time for nodes using the ZMAC scheme when an attack is introduced

Nodes	Packets/sec in bytes	Time in bits/s
5	20480	1357.1
10	35840	1359.5
15	51200	1579.645156
20	66560	1803.241674
25	81920	2072.686908
30	97280	2286.758152
35	112640	3725.497647



Total transmission time using the ZMAC scheme when an attack is introduced

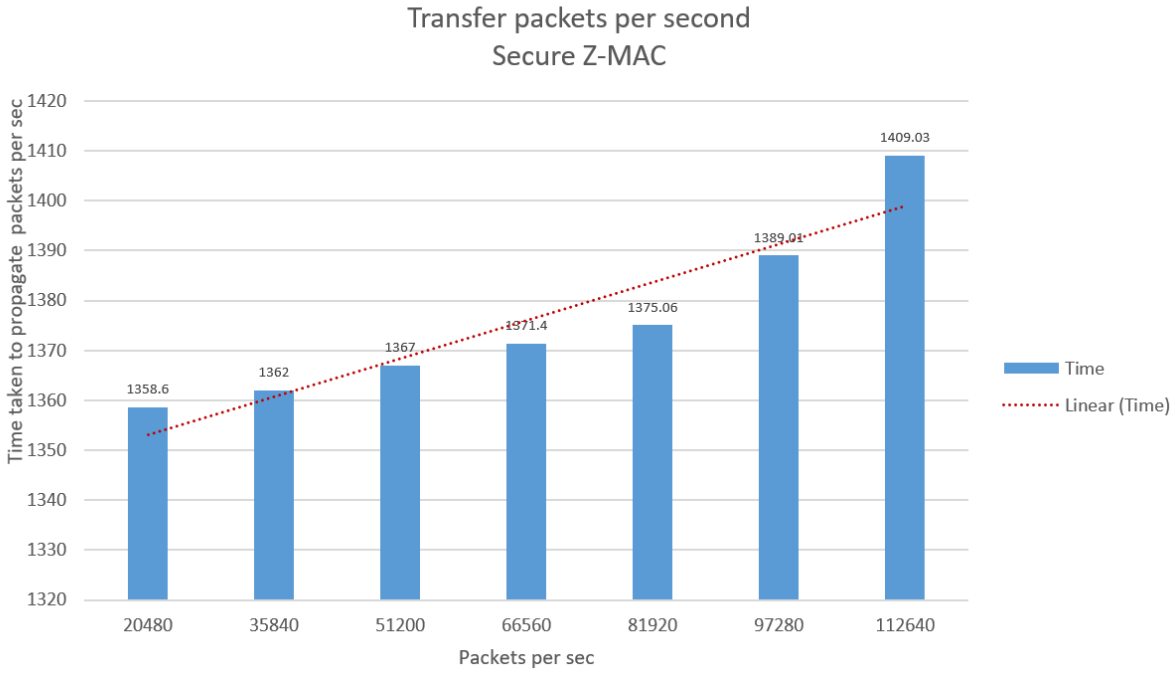
IECI 2021

Results and Discussion – Scenario 3

Total transmission time for nodes using the Secure ZMAC scheme .

Nodes	Packets/sec in bytes	Time in bits/s
5	20480	1358.598129
10	35840	1361.77138
15	51200	1366.963776
20	66560	1371.648392
25	81920	1375.062767
30	97280	1389.011017
35	112640	1409.034265

Total transmission time for nodes using the ZMAC scheme along with IHOP mechanism



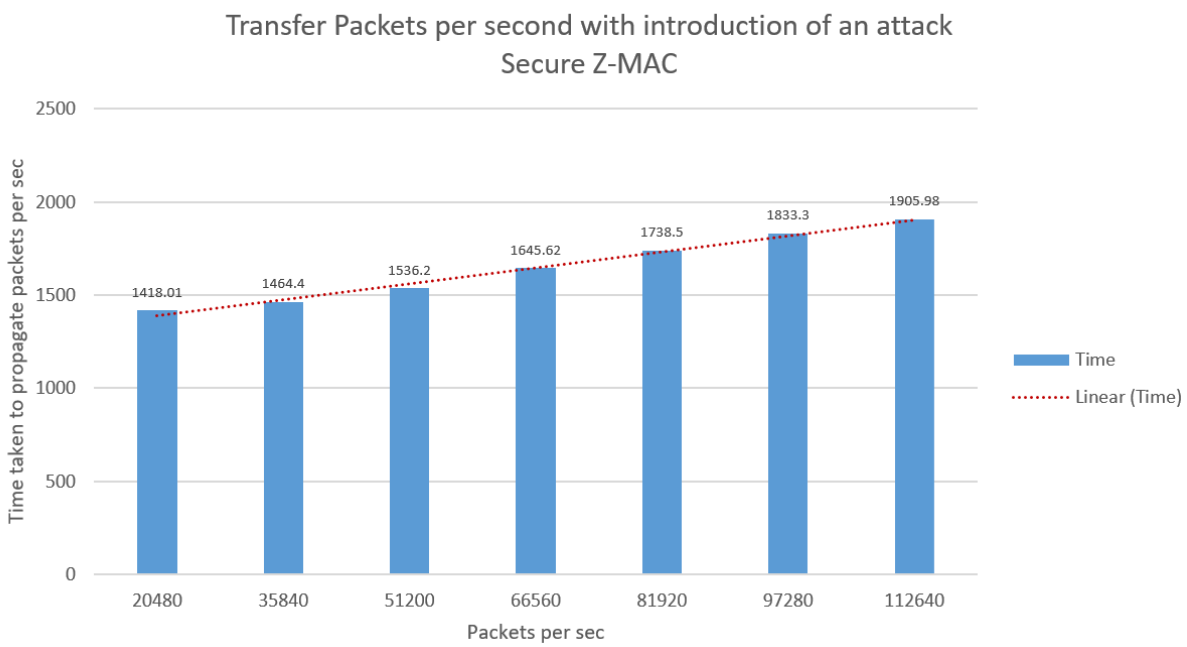
IECI 2021

Results and Discussion

Total transmission time for nodes using the Secure Z-MAC Scheme

Nodes	Packets/sec in bytes	Time in bits/s
5	20480	1418.014112
10	35840	1464.402046
15	51200	1536.198699
20	66560	1645.619443
25	81920	1738.530628
30	97280	1833.294729
35	112640	1905.975264

Total transmission time for nodes using the Secure Z-MAC Scheme



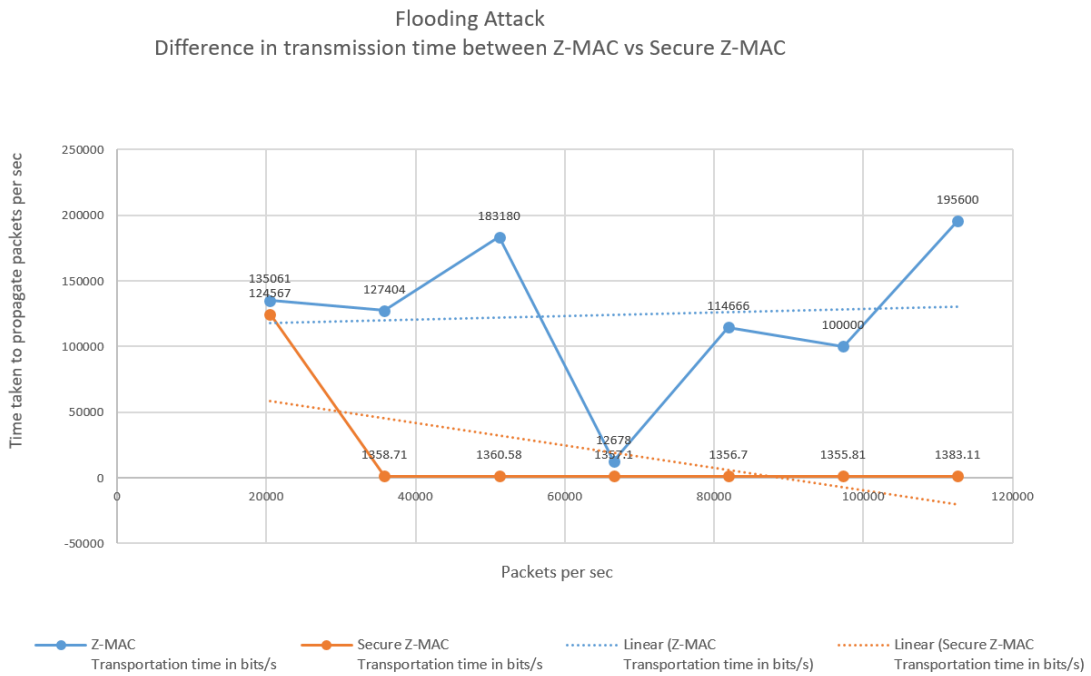
IECI 2021

Results and Discussion

Total transmission time during flooding attack for nodes processed using the secure ZMAC scheme against Z-MAC

Nodes	Packets/ sec in bytes	Z-MAC Transmission time in bits/s	Secure Z-MAC Transmission time in bits/s
5	20480	135061	124567
10	35840	127404	1358.71
15	51200	183180	1360.58
20	66560	12678	1357.1
25	81920	114666	1356.7
30	97280	100000	1355.81
35	112640	195600	1383.11

Graph simulating the transmission time during flooding attack against the packets transmitted in byte in secure Z-MAC scheme against Z-MAC



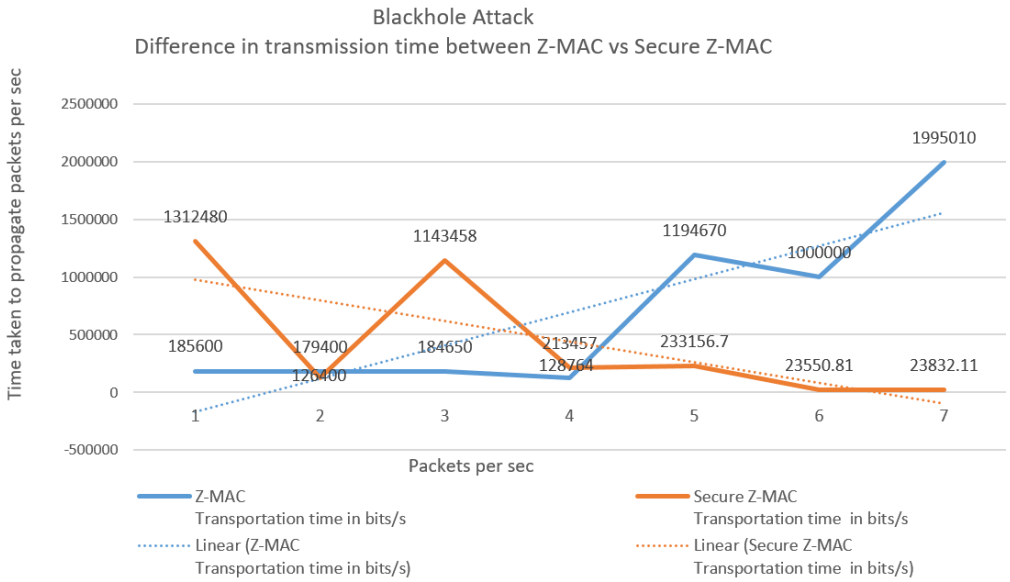
IECI 2021

Results and Discussion

Total transmission time during blackhole attack for nodes processed using the secure ZMAC scheme against Z-MAC

Nodes	Packets/sec in bytes	Z-MAC Transmission time in bits/s	Secure Z-MAC Transmission time in bits/s
5	50480	185600	1312480
10	65840	179400	126400
15	81200	184650	1143458
20	560566	128764	213457
25	781920	1194670	233156.7
30	9007280	1000000	23550.81
35	1001264	1995010	23832.11

Graph simulating the transmission time during blackhole attack against the packets transmitted in byte in secure Z-MAC scheme against Z-MAC

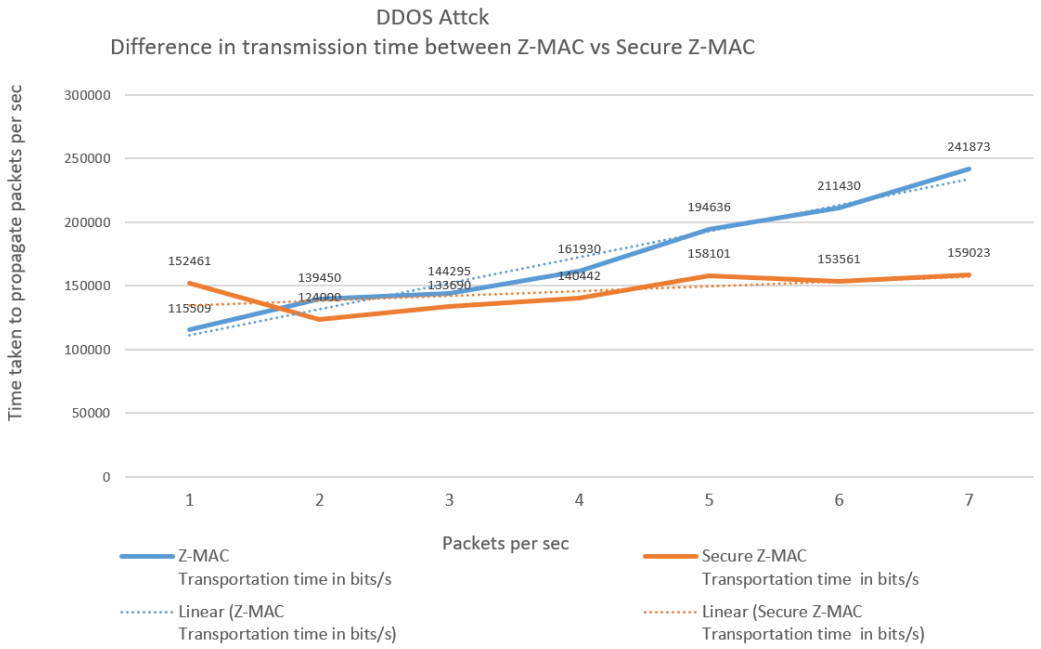


Results and Discussion

Total transmission time during DDOS attack for nodes processed using the secure ZMAC scheme against Z-MAC

Nodes	Packets/sec in bytes	Z-MAC Transmission time in bits/s	Secure Z-MAC Transmission time in bits/s
5	50480	115509	152461
10	65840	139450	124000
15	81200	144295	133690
20	560566	161930	140442
25	781920	194636	158101
30	9007280	211430	153561
35	1001264	241873	159023

Graph simulating the transmission time during DDOS attack against the packets transmitted in byte in secure Z-MAC scheme against Z-MAC



IECI 2021

Results and Discussion

A comparison of Z-MAC and secure Z-MAC protocol

Protocol	Neighbor discovery	Local time Framing(DRAND)	Transmission control(LCL,HCL)	Receiving schedule	Local time synchronization	IHOP	Elliptic curve(Encryption)	Key sharing(Public, Private)	XORING
Z-mac	X	X	X	X	X				
Secure Z-MAC	X	X	X	X	X	X	X	X	X

Results and Discussion

Performance Comparison of Z-MAC and Secure Z-MAC in terms of Flooding, DDOS, and Blackhole Attack.

(Flooding, DDOS, Blackhole) Attack.				
Protocol	Node	Packets	Transmission Time	Network Efficiency
Z-MAC	Identified	Major Lost	Minor Delay	Network Interruption
				Network Delayed
	Compromised	Minor Lost	Major Delay	Network Reliability
		Encrypted Packets		Network Compromised
				Data Integrity
Secure-Z-MAC	Identified	Major Lost	Minor Delay	Network Interruption
				Network Delayed
	Compromised	Minor Lost	Major Delay	Network Reliability
		Encrypted Packets		Network Compromised
				Data Integrity

(Flooding, DDOS, Blackhole) Attack.				
Protocol	Node	Packets	Transmission Time	Network Efficiency
Z-MAC	Identified	Major Lost	Minor Delay	Network Interruption
				Network Delayed
	Compromised	Minor Lost	Major Delay	Network Reliability
		Encrypted Packets		Network Compromised
				Data Integrity
Secure-Z-MAC	Identified	Major Lost	Minor Delay	Network Interruption
				Network Delayed
	Compromised	Minor Lost	Major Delay	Network Reliability
		Encrypted Packets		Network Compromised
				Data Integrity

Results and Discussion

Secure Z-MAC protocol has a higher efficiency, security, and productivity compared to basic Z-MAC protocol. The primary goal of the study was to improve the security of the Z-MAC protocol by making it very safe when used in a wireless network. Additionally, although the network was subjected to a variety of assaults, including flooding, blackhole, and DDOS attacks, it was determined that the secure Z-MAC protocol is securing the network.

Conclusions

Secure Z-MAC protocol was found to be more efficient and secure compared to the basic Z-MAC protocol. Also, the implementation of IHOP mechanism and ECE helped in achieving a higher security for the protocol. For instance, one of the most significant uses of the Secure Z-MAC protocol is Vehicle Area Network, which would aid in boosting vehicular traffic on highways while also improving individual safety and reducing accidents.

Future Plan

- The protocol will be evaluated in the future against a variety of network assaults, including the Sybil, message modification, wormhole, and attacks on the system's multiple levels.

- The future plan calls for the development of hardware or software that implements the proposed secure Z-MAC protocol, enabling the safe transmission of essential communications. The hardware will be connected to the network's user devices through an application, ensuring secure network connection.

Acknowledgments

- I would like to start by thanking the IECI 2021 organizers and board members for giving me the opportunity to participate in this event.

- A special heartfelt thank you to supervisors Professors Dr. Medhat A. Rakha, Dr. Ahmed Alshamy , Dr. Ahmad Mostafa and Dr. Mohammed Fatehy Soliman .

- I would also like to thank my father Nasser AlMansoori, my mother, my husband Khalid AlMansoori, and the rest of my family and friends for their constant support throughout my work. Also special thank you to my daughters and sons for their continuous support.

IECI 2021

Thank you

- **Author Contributions:** Mona Almansoori, Dr.Ahmad Elshamy, and Dr.Ahmad Mustafa, All authors have read and agreed to the published version of the manuscript.

- **Funding:** This research received no external funding.

- **Conflicts of Interest:** The authors declare no conflicts of interest.

Any Comments are welcome

mnmalmansoori@gmail.com

IECI 2021