INTEGRITY VERIFICATION & DATA SECURITY IN WIRELESS SENSOR NETWORKS

[1] Mohammed Amaan Pasha, [2] Mohammed Waheeduddin Hussain, [3] Imtiyaz Khan

[1] PG scholar, Shadan College of Engineering and Technology

[2] Professor, Dept.of Information Technology, Shadan College of Engineering and Technology

[3] Professor Dept of Information Technology, Shadan College of Engineering and Technology

Abstract: The project aims to enhance the security of wireless sensor networks used in monitoring applications by addressing vulnerabilities related to data integrity and confidentiality. The proposed solution integrates a Chaotic technique for data integrity verification, where a verification hash code is sent along with encrypted messages. Additionally, homomorphic encryption is employed to ensure the confidentiality of the transmitted data. The system comprises a sender functionality is responsible for selecting source and destination, generating secret keys, calculating integrity codes, encrypting messages, and transmitting them to the receiver. The receiver functionality receives the encrypted message along with the integrity code, decrypts the message, regenerates the integrity code, and verifies its match with the received code for successful verification. 5. By combining these techniques, the project provides a robust defense mechanism against potential attacks, ensuring the integrity and security of data transmitted through wireless sensor networks in various monitoring applications.

Index terms - *Wireless Sensor Networks (WSNs), IOT, Integrity, privacy, Security, sensor networks.*

1. INTRODUCTION

Wireless sensor network (WSN) [16] refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. [1] WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. The increased adoption of wireless sensors across industry is due, like most industrial technologies, to solid, practical reasons. Chief among these reasons is ease of implementation (no long cable runs), ability to operate in harsh environments, easy troubleshooting and repair, and high levels of performance. If you've been following the adoption of wireless sensor networks in industry at any level, you're bound to be aware of their prevalence in the oil and gas and water/wastewater industries—especially for use in tank farm and wellhead monitoring, where traditional wired communication is simply too costly when compared to wireless. Stories of wireless sensor successes in these applications abound.

Over The fundamental problem for a two-tired sensor network [2] is the following: How can we design the storage scheme and the query protocol in a privacy- and integrity-preserving manner?

A satisfactory solution to this problem should meet the following two requirements.

1) Data and query privacy: Data privacy means that a storage node cannot know the actual values of sensor collected data. This ensures that an attacker cannot understand the data stored on a compromised storage node. Query privacy means that a storage node cannot know the actual value of sink issued queries. This ensures that an attacker cannot understand, or deduce useful information from, the queries that a compromised storage node receives.

2) Data integrity [3]: If a query result that a storage node sends to the sink includes forged data or excludes legitimate data, the query result is guaranteed to be detected by the sink as invalid. Besides these two hard requirements, a desirable solution should have low power and space consumption because these wireless devices have limited resources.

Wireless Sensor Network (WSN) [1, 2] consists of mostly tiny, resource-constraint, simple sensor nodes, which communicate wirelessly and form ad hoc networks in order to perform some specific operation. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Simplicity in WSN with resource constrained nodes makes them very much vulnerable to variety of attacks. The attackers can eavesdrop on its communication channel, inject bits in the channel, replay previously stored packets and much more. An adversary can easily retrieve valuable data from the transmitted packets that are sent (Eavesdropping). That adversary can also simply intercept and modify the packets' content meant for the base station or intermediate nodes (Message Modification), or retransmit the contents of those packets at a later time (Message Replay). Finally, the attacker can send out false data into the network, maybe masquerading as one of the sensors, with the objectives of corrupting the collected sensors' reading or disrupting the internal control data (Message Injection). Securing the WSN needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar or more hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. The sensor nodes may not be tamper resistant and if an adversary compromises a node, it can extract all key material, data, and code stored on that node. As a result, WSN has to face multiple threats that may easily hinder its functionality and nullify the benefits of using its services.

2. LITERATURE SURVEY

Wireless Sensor Networks (WSN) [2] is a rising technology that proves enormous assurance in various applications. The combination of

communication processing and sensing technology provides profitable low cost and efficient environment for different systems. The small nodes constrained capabilities to collect, process, sense and disseminate data for applications. The intent of this paper [1] is to investigate the architecture of traditional sensor and components. Further, discuss standards and applications, which are used in industrial zone, discuss some technologies of industrial applications such as Zigbee, wirelessHART, ISA 100 and compare with each other. We shed some light on the future trends as well.

The emergence of wireless sensor networks (WSN) [24] as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues, the challenges and to propose some solutions to secure the WSN against these security threats. While the set of challenges in sensor networks are diverse, this paper focus only on the challenges related to the security of Wireless Sensor Network. [2] This paper begins by introducing the concept of Wireless Sensor Network (WSN). The introductory section gives brief information on the WSN components and its architecture. Then it deals with some of the major security issues over wireless sensor networks (WSNs) [20]. This paper also proposes some of the security goal for Wireless Sensor Network. Further, as security being vital to the acceptance and use of sensor networks for many applications; I have made an in depth threat analysis of Wireless Sensor Network. Lastly it proposes some security mechanisms against these threats in Wireless Sensor Network.

The wireless sensor networks [22, 23] have several applications in different areas like medical, military, industry, safety, etc. Recently, Kumari and Om have discussed an authentication protocol for wireless sensor networks in coal mines for safety monitoring. In this paper [3], we cryptanalyze their scheme and find that it is vulnerable to the smart card loss attack, stolen verifier attack, and denial of service attack, besides other problems: (1) user traceability and (2) the sensor nodes are not anonymous. Here, we purpose an improved scheme by overcoming these limitations. We formally show the security analysis of our proposed scheme using random oracle and its security verification using the AVISPA tool. We carry out its informal analysis to show its resistivity to various known attacks. It requires less computational and storage costs, and is more secured than the related schemes. We also show its practical demonstration using NS2 simulator.

A wireless sensor network (WSN) [29, 32] has important applications such as remote environmental monitoring and target tracking. In addition, Wireless Sensor networks is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. [4] This has been enabled by the availability for a kind of possible attacks; the innate power and recall limit of sensor nodes earn customary security solutions unfeasible. These

sensors are equipped with wireless interfaces with which they can communicate with one pther to form a network. In this paper we present a survey of security issues in WSNs, address the state of the art in research on sensor network security, and discuss some future directions for research.

Networking together hundreds or thousands of cheap microsensor nodes allows users to accurately monitor a remote environment by intelligently combining the data from the individual nodes. These networks require robust wireless communication protocols that are energy efficient and provide low latency. [5] We develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for microsensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. [5] LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. Our results show that LEACH can improve system lifetime by an order of magnitude compared with general-purpose multihop approaches.

3. METHODOLOGY

i) Proposed Work:

The proposed system enhances wireless sensor network (WSN) [17] security by integrating Chaotic Hashcode Integrity Algorithm for data integrity verification and Homomorphic encryption for improved data security. This approach mitigates the risks associated with key exposure in traditional encryption, ensuring secure and accurate data transmission in WSN applications [19] such as traffic monitoring and home surveillance. The proposed system employs the Chaotic Hashcode Integrity Algorithm, providing a more robust and reliable method for data integrity verification, ensuring that the received data has not been tampered with during transmission. Homomorphic encryption in the proposed system enhances data security by allowing computations on encrypted data without the need for decryption. This protects sensitive information from exposure even if the encryption keys are compromised. Unlike the existing system, the proposed system minimizes the risks associated with key exposure by combining encryption with Chaotic Hashcode Integrity. This ensures that even if an attacker gains access to the encryption key, the integrity of the data can still be verified through the hashcode. The proposed system allows for the generation of dynamic and adaptable wireless sensor networks, facilitating efficient communication between nodes. This adaptability improves the overall responsiveness and reliability of the system in various monitoring applications.

ii) System Architecture:

The proposed architecture enhances the privacy, integrity and security also affect the Quality of service in Wireless Sensor Network. Quality of Service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. QoS is sometimes used as a quality

measure, with many alternative definitions, rather than referring to the ability to reserve resources. Quality of service sometimes refers to the level of quality of service, i.e. the guaranteed service quality. High QoS is often confused with a high level of performance or achieved service quality, for example high bit rate, low latency and low bit error probability.

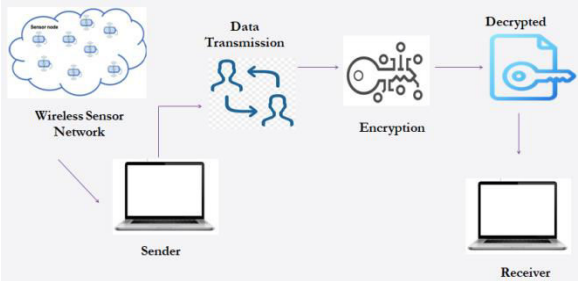

Fig 1 Proposed Architecture

iii) Processing:

1. Wireless Sensor Networks (WSN) [20, 22]:

Consist of small sensor devices dispersed in the environment.

Sensors collect data from the surroundings, e.g., for road traffic or home monitoring.

2. Sender:

Initiates communication, selecting a source and destination.

He Generates a secret key for encryption. And send the data

Sender Uses Chaotic technique to calculate an integrity code.

Encrypts sensor data and integrity code for secure transmission**.**

3. Encrypted Data Transfer:

data is Transmitted in encrypted way securely through the wireless sensor network using IoT connections [21, 25, 30, 31].

4. Decrypted Data:

Receiver receives and decrypts the transmitted data using the secret key [12, 13].

5. Receiver:

Verifies data integrity by regenerating the integrity code from the decrypted message. He Compares received and regenerated codes for verification. Successful verification ensures the reliability of the decrypted data..

vi) Modules:

1. Generate Network:

- This module creates a wireless sensor network (WSN) by generating nodes within the simulation environment.

- Each node represents a device in the network, and their connections form the communication infrastructure.

- The purpose is to establish the framework for data transmission within the WSN [16].

2. Source Node:

- Users select a specific node within the WSN to act as the source of the data transmission.

- This module allows users to designate the origin point for sending information within the network.

3. Destination Node:

- Users specify a destination node where the data will be transmitted from the source node.

- This module defines the endpoint for the data to reach within the WSN [32].

4. Secret Message:

- Users enter a confidential message that needs to be transmitted from the source to the destination.

- This module involves inputting the sensitive information that requires secure transmission through the WSN.

5. Send Data:

- After setting up the network, source node, destination node, and secret message, this module initiates the process of encrypting and transmitting the data.

- The system utilizes encryption techniques, Chaotic Hashcode Integrity Algorithm, and Homomorphic encryption, to secure the message during transmission.

- The encrypted data is then sent through the WSN to the specified destination node.

4. EXPERIMENTAL RESULTS

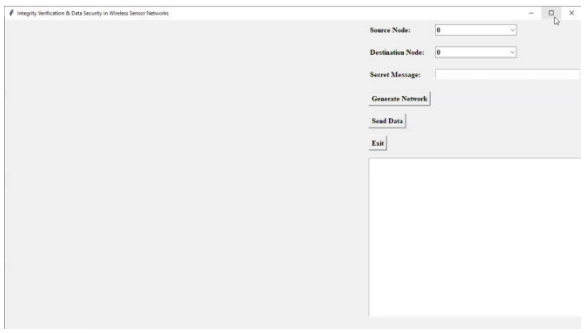

Fig 2 User interface

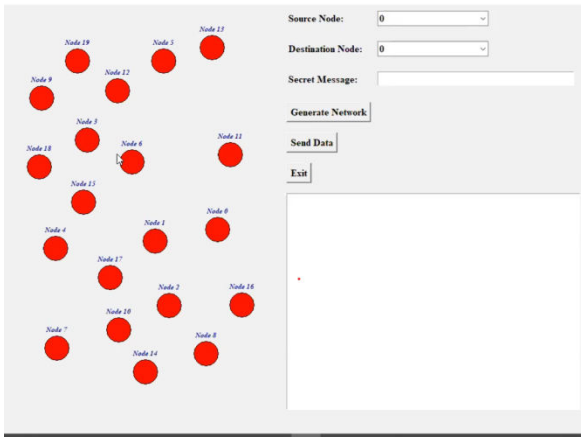

Fig 3 Generate network

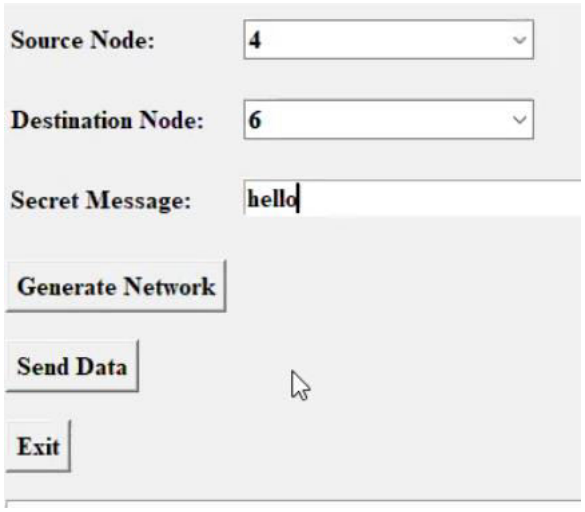

Fig 4 User input selection

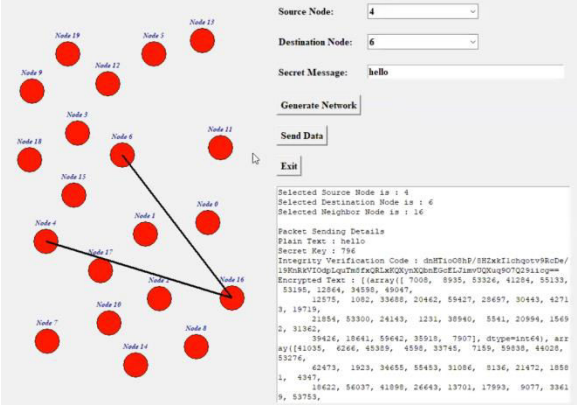

Fig 5 Send data

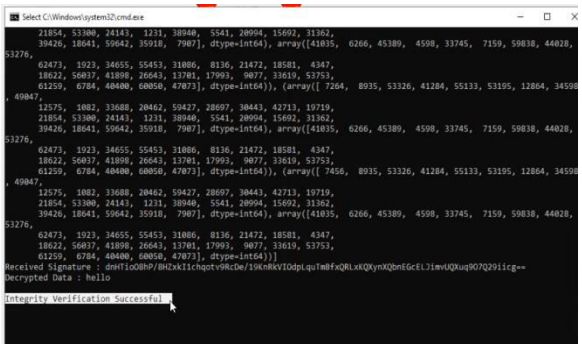

Fig 6 Result in console

5. CONCLUSION

The integration of the Chaotic Hashcode Integrity Algorithm and Homomorphic encryption in this project significantly enhances the security of wireless sensor networks (WSNs) [1, 2]. These measures provide robust data integrity verification and protection against potential key exposure, mitigating vulnerabilities present in traditional encryption methods. The implementation of dynamic network adaptability ensures flexibility and responsiveness within the WSN. This feature allows for efficient communication between nodes, adapting to changing conditions and improving the overall reliability of the system across various monitoring applications. The seamless integration of modules like "Generate Network," "Source Node," "Destination Node," "Secret Message," and "Send Data" streamlines the data transmission process. This efficiency ensures that users can easily configure and transmit data within the wireless sensor network, reducing the complexity often associated with secure communication protocols By addressing key exposure risks, implementing advanced encryption techniques, and ensuring data integrity verification, this project establishes a comprehensive approach to data security in WSNs [16]. The synergistic integration of these features creates a robust system capable of safeguarding sensitive information in real-world monitoring scenarios.

6. FUTURE SCOPE

Investigate and implement quantum-safe cryptographic algorithms to future-proof the system against potential threats from quantum computing. This would ensure the continued security of the wireless sensor network in the face of evolving technologies. Extend the project by incorporating edge computing capabilities within the wireless sensor network [30, 32]. This would enable real-time processing of data at the network's edge, reducing latency and enhancing overall system efficiency for time-sensitive applications. Develop mechanisms for dynamic reconfiguration of the wireless sensor network in response to changing security conditions. This could involve adaptive routing algorithms, self-healing networks, and dynamic adjustments to encryption protocols based on the perceived security threats in real-time. Investigate methods to optimize the proposed system for resource-constrained devices commonly found in wireless sensor networks. This may involve developing lightweight encryption

techniques and algorithms to minimize computational overhead and energy consumption.

REFERENCES

[1] K.N. Qureshi, A.H. Abdullah, Adaptation of wireless sensor network in industries and their architecture, standards and applications, World Appl. Sci. J. 30 (10) (2014) 1218–1223.

[2] V. Kumar, A. Jain, P. Barwal, Wireless sensor networks: security issues, challenges and solutions, Int. J. Inf. Comput. Technol 4 (8) (2014) 859–868.

[3] D. Kumar, S. Chand, B. Kumar, Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines, J. Ambient Intell. Humaniz. Comput. 10 (2) (2019) 641–660.

[4] P.B. Hari, S.N. Singh, Security issues in wireless sensor networks: current research and challenges, in: Paper presented at the 2016 international conference on advances in computing, communication, & automation (ICACCA) (Spring), 2016.

[5] W. Heinzelman,"Application Specific Protocol Architecture for Wireless Sensor Networks", B.S., Cornell University 1995, M.S. Massachusetts Institute of Technology (1997) at MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT) June 2000.

[6] G. Singh, Supriya,, A study of encryption algorithms (RSA, DES, 3DES and AES) for information security, Int. J. Comput. Appl. 67 (19) (2013) 33–38.

[7] W. Burr, Selecting the advanced encryption standard, IEEE Secur. Priv. 1 (2) (2003) 43–52.

[8] M. Frunza, Gh. Asachi, Improved RSA encryption algorithm for increased security of wireless networks, in: ISSCS International Symposium,vol. 2, 2007.

[9] R. Kodali, N. Sarma, Energy efficient ECC encryption using ECDH, Lecture Notes in Electrical Engineering, vol. 248, Springer, 2013, pp. 471–478.

[10] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), Int. J. Inf. Secur. 1 (1) (2001) 36– 63.

[11] M. Balitanas, WiFi protected access-pre-shared key hybrid algorithm. Int. J. Adv. Sci. Technol., 2009, 12.

[12] S. Karthik, A. Muruganandam, Data encryption and decryption by using triple DES and performance analysis of crypto system, Int. J. Scient. Eng. Res. (IJSER), ISSN (Online) 2 (11) (2014) 2347–3878.

[13] J.D. Gaur, A. Kumar Singh, N.P. Singh, G.V. Rajan, ''Comparative study on different encryption and decryption algorithm, in: 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2021, pp. 903-908, doi: 10.1109/ ICACITE51222.2021.9404734.

[14] S.K. Verma, D.B. Dr, Ojha, A discussion on elliptic curve cryptography and its applications, JCSI Int. J. Comput. Sci. Issues Vol. 9, Issue 1, No 1 (2012), ISSN (Online): 1694–0814.

[15] X. Zhang, X. Wang, Digital image encryption algorithm based on elliptic curve public cryptosystem, IEEE Access 6 (2018) 70025–70034.

[16] A. Dutta, K. Naveen Kumar, N. Sai, R.R. Chintala, An efficient light weight cryptography algorithm scheme for WSN devices using chaotic map and GE, Int. J. Pure Appl. Math. 118 (20) (2018) 861–875.

[17] S. Ozdemir, H. Ichakawa et al. (Eds.), Secure and reliable data aggregation for wireless sensor networks, LNCS 4836, pp. 102– 109 (2009).

[18] Z. Dawahdeh, N.S. Yaakob, A new modification for menezesvanstone elliptic curve cryptosystem, J. Theor. Appl. Inf. Technol. 85 (2016) 290–297.

[19] elena Misic, Vojislav Misic,, Wireless personal area networks performance interconnections and security with, John Wiley & Sons Ltd, 2008, IEEE 802.15.4.,.

[20] Nandigama, N. C. (2025). Leveraging ChatGPT for multi-language data engineering code generation in distributed analytics systems. Journal of Informatics Education and Research, 5(3). https://doi.org/10.52783/jier.v5i3.3370.

[21] M.I. Sobhy, A.-E. Shehata, Methods of attacking chaotic encryption and countermeasures, in: 2001 IEEE international conference on acoustics, speech, and signal processing, Salt Lake City, UT, 7–11 May 2001, pp.1001–1004. New York: IEEE.

[22] M. Panda, Security in wireless sensor network using cryptography techniques, Am. J. Eng. Res. (AJER) 3 (2014) 50–56.

[23] M. Rajput, U. Ghawte, Security challenges in wireless sensor networks, Int. J. Comput. Appl. 168 (2017) 24–29.

[24] H. Yetgin, K.T.K. Cheung, M. El-Hajjar, L.H. Hanzo, A survey of network lifetime maximization techniques in wireless sensor networks, IEEE Commun. Surv. Tutor. 19 (2) (2017) 828–854.

[25] Naga Charan Nandigama,"A Hybrid Big Data And Cloud-Based Machine Learning Framework For Financial Fraud Detection Using Value-At-Risk", Ijrar - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P-ISSN 2349-5138, Volume.11, Issue 3, Page No pp.901-905, September 2024, Available at : http://www.ijrar.org/IJRAR24C3021.pdf

[26] A. Gyrard, M. Serrano, Connected Smart Cities: Interoperability with SEG 3.0 for the Internet of Things, in: 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016, pp. 796-802, doi: 10.1109/WAINA.2016.151.

[27] S. De, P. Barnaghi, M. Bauer, S. Meissner, Service modelling for the Internet of Things, Federated Conf. Comput. Sci. Inform. Syst. (FedCSIS) 2011 (2011) 949–955.

[28] S. Subasree, N.K. Sakthivel, Design of a new security protocol using hybrid cryptography algorithmsk, IJRRAS. 2 (2) (2010) 95–103.

[29] N. Kumar, A secure communication wireless sensor networks through hybrid (AES+ECC) algorithmk, Vol. 386, von LAP LAMBERT Academic Publishing, Koln, Germany, 2012.

[30] W. Ren, Z. Miao, A hybrid encryption algorithm based on DES and RSA in Bluetooth Communication, in: 2010 Second International Conference on Modeling, Simulation and

Visualization Methods, 2010, pp. 221-225, doi:10.1109/ WMSVM.2010.48.

[31] D.E. Ramaraj, S. Karthikeyan, M. Hemalatha, A design of security protocol using hybrid encryption technique (AESRijndael and RSA), Int. J. Comput. Internet Manag. 17 (1) (2009) 78–86.

[32] H. Tange, B. Andersen Attacks and countermeasures on AES and ECC, IN: 2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), 2013, pp. 1-5.