www.revistageintec.net
ISSN: 2237-0722

revista GEINTEC
Gestão, Inovação e Tecnologias

Security Enhancement in Data Propagation for Wireless Network

M.D. Zainlabuddin[1]; Dr. Neeraj Sharma[2]

[1]Research Scholar, Dept. of Computer Science & Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.

[2]Research Guide, Dept. of Computer Science & Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.

Abstract

Wireless communication technology is rapidly progressing due to its high quality and high speed of information transfer from one location to another. It is necessary to ensure the safety of wireless sensor networks with this progress. One of the main security concerns in WSNs is eavesdropping, an intrusion that collects information from other devices across the network. Eavesdropping attacks are insidious and it is hard to realise that they happen. When connected with a network, users can feed sensitive information inadvertently, such as passwords, account numbers, browsing, email content, etc. Security improvement in wireless network communication is therefore required.

Key-words: Security Enhancement, Wireless Network, Eavesdropping Attacks.

1. Introduction

In contemporary network environments, security is a key concern. Early on, protocols implicitly believed that the trustworthy and altruistic users will never try to snoop on routed traffic and pick up passwords for plaintext, fake an address on the sender of an incoming email message, or try to subvert name services or end hosts. If a network or internetwork is used by a single organisation and a small group of academic organisations who have a common goal and interest and are unified by a common ethic, it may be an acceptable idea; when the network is expanded into the real world, with users with rivalrous ideologies and interests, such conclusions are questionable.

Although the intended users of a WSN device can't compete with one another (the ones responsible for the implementation are either end users or agents for them), external attackers have enough opportunity to interfere with the traffic sent through unsafe multihop channels. External attackers would be required to compromise the existence of physical channels in wired networks. For example, a backbone cable splicing entails visible fixations and potentially traceable effects on the channel characteristics and reception. In WSN, however, the deployment area is always diminished and any arbitrary external device with a transceiver can reach the wireless channel. This provides vulnerability to malicious attacks by external actors and thus a system security risk.

Wireless Networks

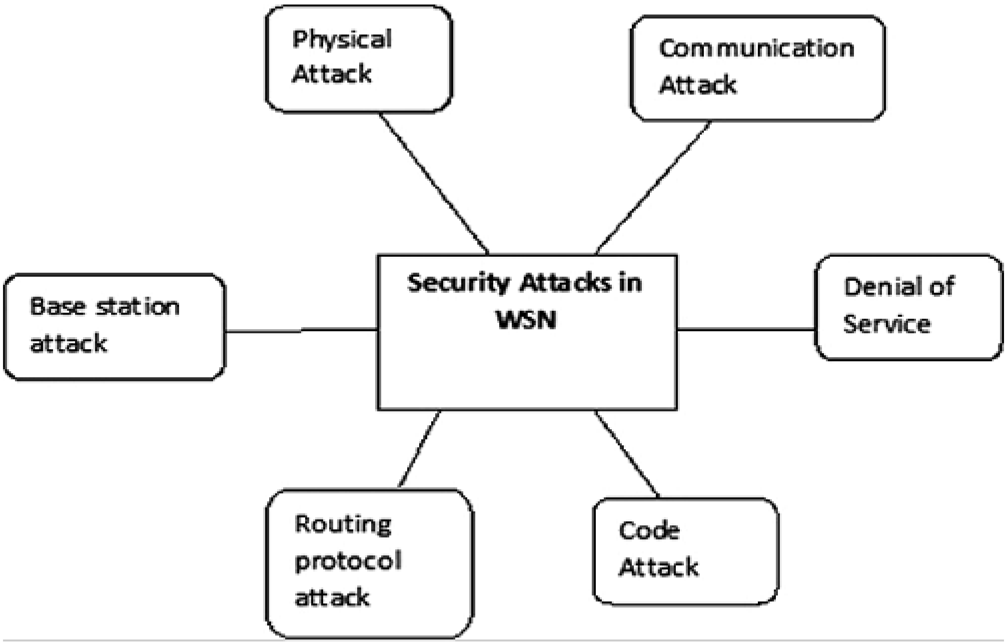
Wireless networks are essentially used as the medium for transportation between devices, between devices and conventional wired networks. Wireless networks are numerous and varied, but are mostly divided into three categories based on their coverage. Networks for Wireless Wide Area (WWAN), Wireless Wireless and Personal Area Networks (WPAN).

Popular technologies can be categorised into various categories by service range. Telecommunications companies have made considerable progress worldwide in transporting voice and data traffic through their cellular networks; however, the next generation infrastructure under development around the world is designed to provide improved multimedia traffic capacity and efficiency. WiMAX (IEEE 802.16) is able to provide users with high-speed wireless Internet access in a metropolitan area. Wireless internet (IEEE 802.11) allows users to link to a company or campus building via a local location. In addition, Bluetooth (IEEE 802.15) can provide low-cost and short-range communication for portable devices in a personal area (often less than 10 metres).

2. Need for Security

Wireless LANS is increasingly recognised as a generalised networking alternative for a wide variety of business customers. But one of the main disadvantages is that the wireless LANs are unsafe and the data they transmit can easily be broken and changed. In wireless networks protection is much more important and mandatory than wired networks simply because when data is transferred to the neighbourhood over the wireless network, it is actually broadcast. Without such countermeasures, the wireless systems can not be used where sensitive data is transmitted over the airwaves. In all wireless systems, a definite and precise degree of protection is mandatory. If sensitive data such as that from financial institutions' networks, banks, military networks, or terrorist data etc. were transmitted through the wireless system, then extra privacy and confidentiality precautions should be taken, otherwise one can imagine how useful things are risky.

Fig. 1 - Security Issues in Wireless Sensor Network



3. Security Requirements

The security situation in a general network system is different depending on different applications, including confidentiality and integrity of data, authentication and availability.

Data Confidentiality and Integrity: For any message sent, the MUST network provides strong data security, honesty and replay protection. Data confidentiality and integrity help create a protected communication channel for the user in an unsafe environment, allowing only interacting users to understand the messages received, produce or change valid messages. In addition, replayed messages should be remembered and discarded, while the honesty check may be passed. The well-designed cryptography functions and effective replay security techniques can be met these requirements.

Mutual Authentication: The MUST network provides mutual authentication, which means the talking people authenticate the identity of each other. If required, the authentication method should also be combined with key generation, distribution and management to provide the cryptographic mechanism with secret keys. Flexible permission and access control policies may be deployed to restrain users' privileges based on the authentication performance.

Availability: Availability is another essential category of safety criteria and is a type of robustness. The network should be able to prevent an opponent from disconnecting a legitimate person or the whole machine. In other words, Denial of Service (DoS) attacks or, at least, mitigated attacks should be removed.

4. Review of the Literature

Yi Lu et al discussed in her thesis with the title "Secure wireless systems with versatile base stations" on the WANET network and the wireless network and proposed networks HMWN (Hierarchical Mobile wireless) for their support for portable base stations, In this context, secure parcel shipping calculations and confirmations as well as the most important exchanged agreements are forwarded to secure the basis of the systems.

Golle, P. Greene et al in their work entitled " Detecting and Correcting Malicious Information in VANET", the designers vigorously adhere to the hub hub of communication, which, due to the trade in taking harmful information. At the same time, easy access to data managed by VANET networks is likely to increase the problematic security goal of the information approval. In addition, they proposed a general method for assessing the legitimacy of VANET information. In their methodology, a concentrator seeks possible clarifications for the information gathered, based on how harmful concentrators may be available. Explanations that are reliable for the VANET network hub model are provided, and the hub recognizes the information listed in the most important notes on logging. Our methods for creating and evaluating clarifications are based on two assumptions: first; Hubs can tell at least some hubs that are separated from each other and from the second. Controversy over greed reflects precisely a malicious behavior in a VANET, it legitimizes both assumptions and shows our methodology on explicit VANET.

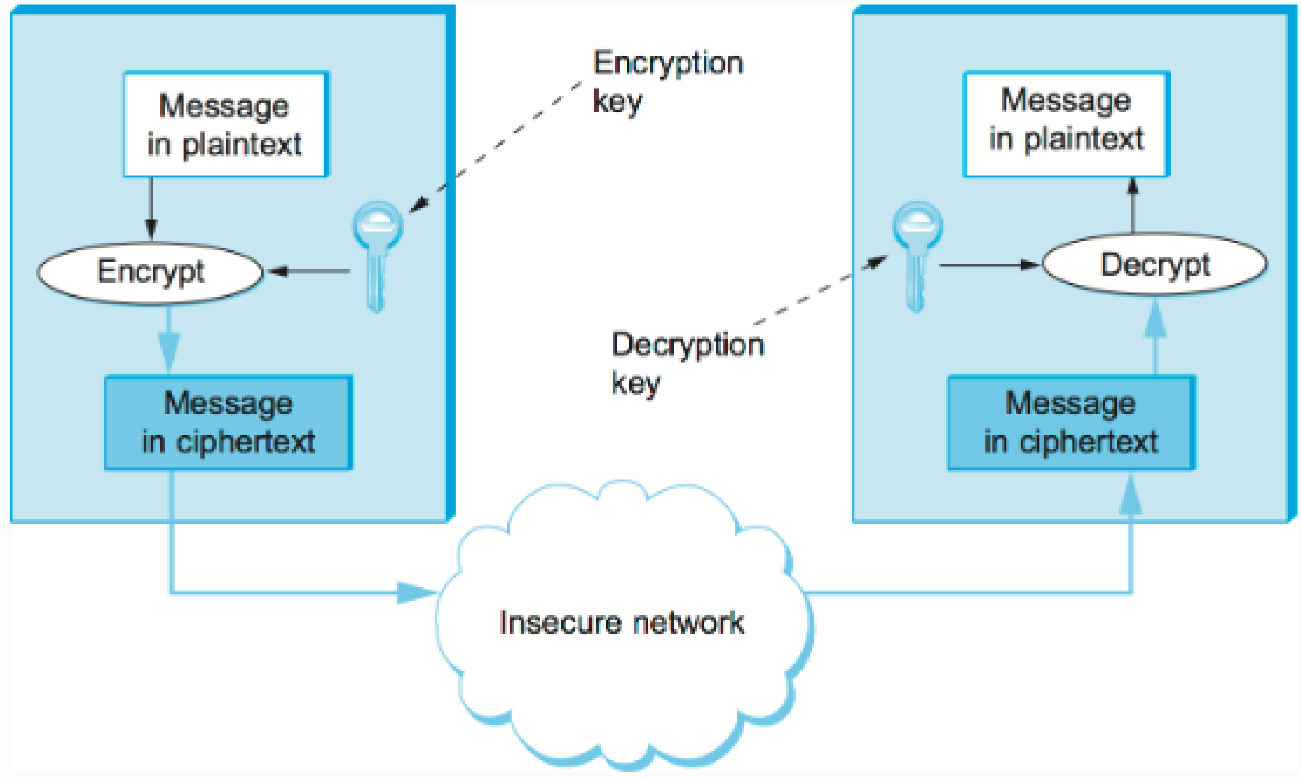
Rouba El Kaissi's et al in their work entitled " DAWWSEN: A Defense Mechanism Against Wormhole Attacks in Wireless Sensor Networks", the designer presented and proposed an item protecting against wormhole attacks in wireless sensor systems. In particular, a basic convention for the steering shaft is proposed and demonstrated as effective protection against wormhole attacks by ns-2 recovery. In addition, they found another convention DAWWSEN consolidation a system of recognition and called barrier against the onslaught of wormholes, an innovative attack that produces real results in leadership conventions sensors. DAWWSEN is characterized by the fact that it requires no topographic data sensor hub and does not use the timestamp of the packet identified as a method of making a wormhole attack that is important to the compulsory nature of the assets of the sensor concentrators.

5. Proposed Methodology

Cipher Block Strategy

CBS is the most common block mode to generate cypher blocks using 64-bit fixed plaintext blocks. For the first block of plaintext an initialising vector (IV) is used in CBS. While encrypting, each plaintext block is XOR -ed with the previous cypher text block until encryption and the XOR is decrypted after the cypher text block has been decrypted. Two formulas for encryption and decryption are used here.

Fig. 2 - Cipher Block



Algorithm

```
from Crypto import Random
from Crypto.Cipher import CBS
def encrypt(plaintext):
# initialize CBS
random = Random.new()
```

```
iv = random.read(16)
key = random.read(16)
cbs = CBS.new(key, CBS.MODE_CBC, iv)
# add PKCS#7 padding
pad = 16 - len(plaintext) % 16
plaintext += bytes([pad] * pad)
# encrypt
ciphertext = iv + cbs.encrypt(plaintext) return key, ciphertext
def decrypt(ciphertext, key):
# initialize CBS
iv = ciphertext[:16]
cbs = CBS.new(key, CBS.MODE_CBC, iv)
# decrypt
plaintext = cbs.decrypt(ciphertext[16:])
# padding
pad = plaintext[-1]
if pad not in range(1, 17):
raise Exception()
if plaintext[-pad:] != bytes([pad] * pad):
raise Exception()
# remove padding
return plaintext[:-pad]
```

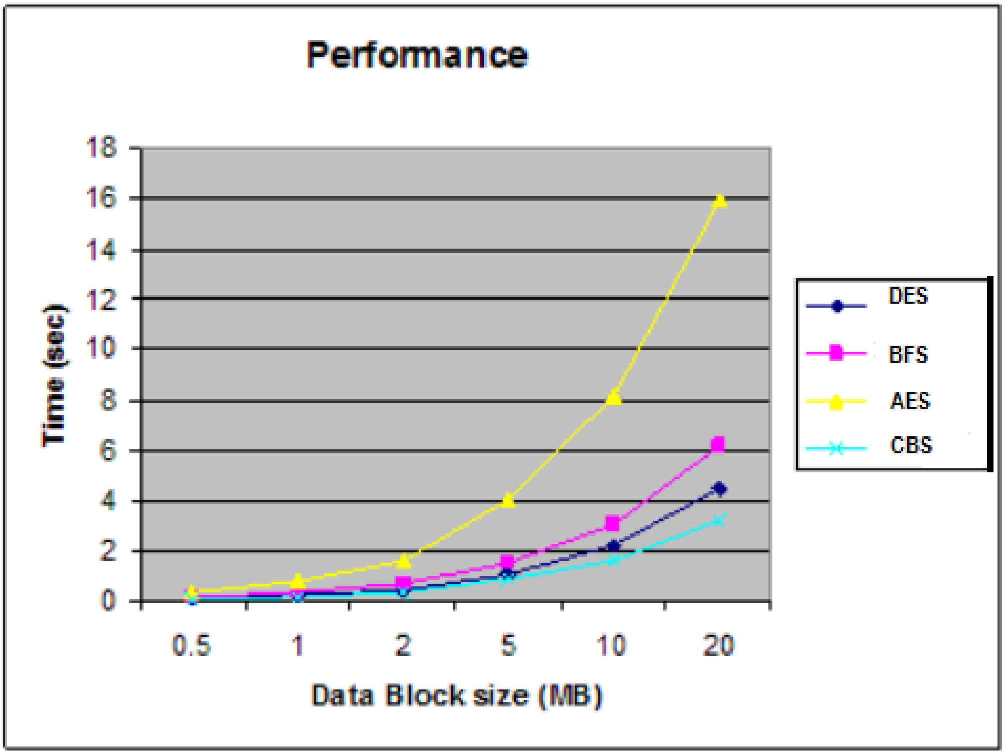
Advantages of CBS Mode

Parallel encryption is limited in CBS, as the encryption process cannot be processed before the previous message block is encrypted and the following encryption process is passed on. Although this is an inconvenience in the chip block strategy mode, this block chip mode has several advantages that are listed below. Firstly, it's simple to enforce this mode of operation and less complex.

6. Result

Due to its key chain structure, AES takes more processing time than CBS. The findings shown in Figure 3 also show that for many applications the added additional time is not important since CBS is much better than AES in terms of security.

Fig. 3 - Comparison of Performance CBS



Encryption Decryption Time Performance

The runtime of encryption algorithms, for each message-size, is compared in Figure 4. The simulation was carried out in multiple sizes. AES was marginally better than CBS. It can be observed. In every case, the AES encryption was completed within a smaller period of time. The gap begins to increase in the largest size of the file, about 65 bytes. As the size of the message continues to rise, this distance further increases the disparity between the algorithms.

There is, however, a small difference in decryption time. Figure 5 illustrates the average algorithms decryption time. AES achieves a slight advantage over CBS with small messages. However, CBS is showing better results than AES as the file size increases.

Fig. 4 - Average Encryption Time

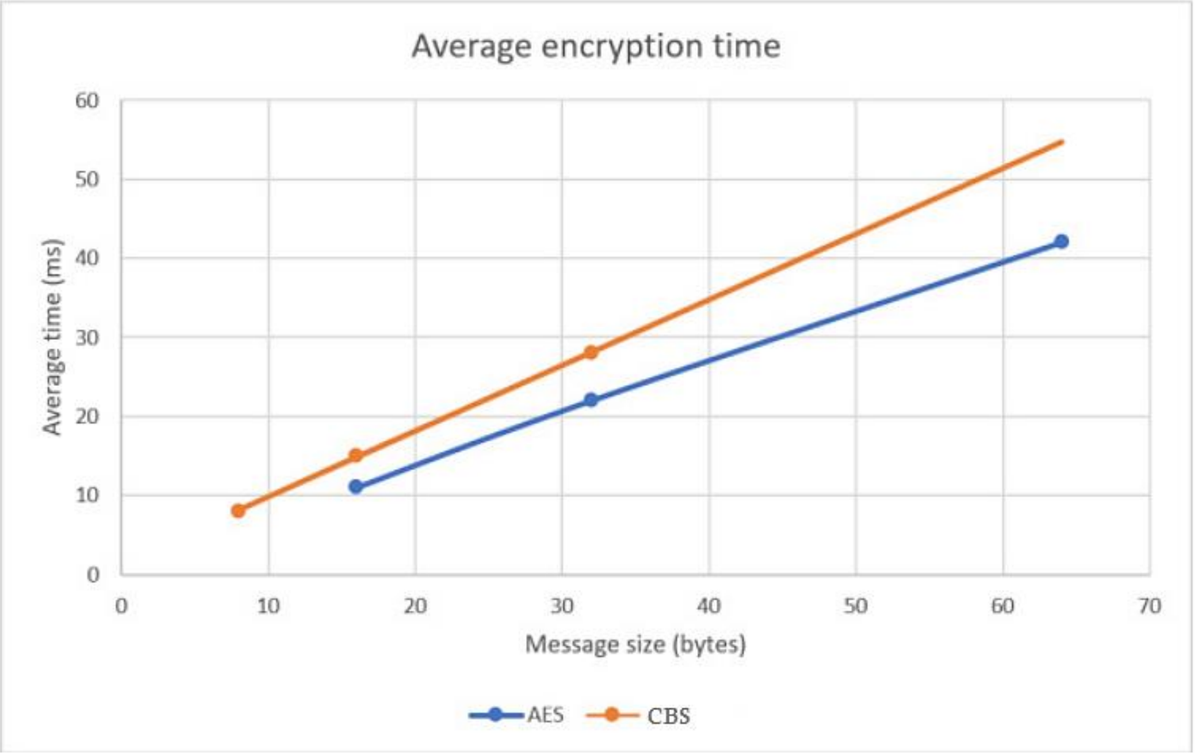
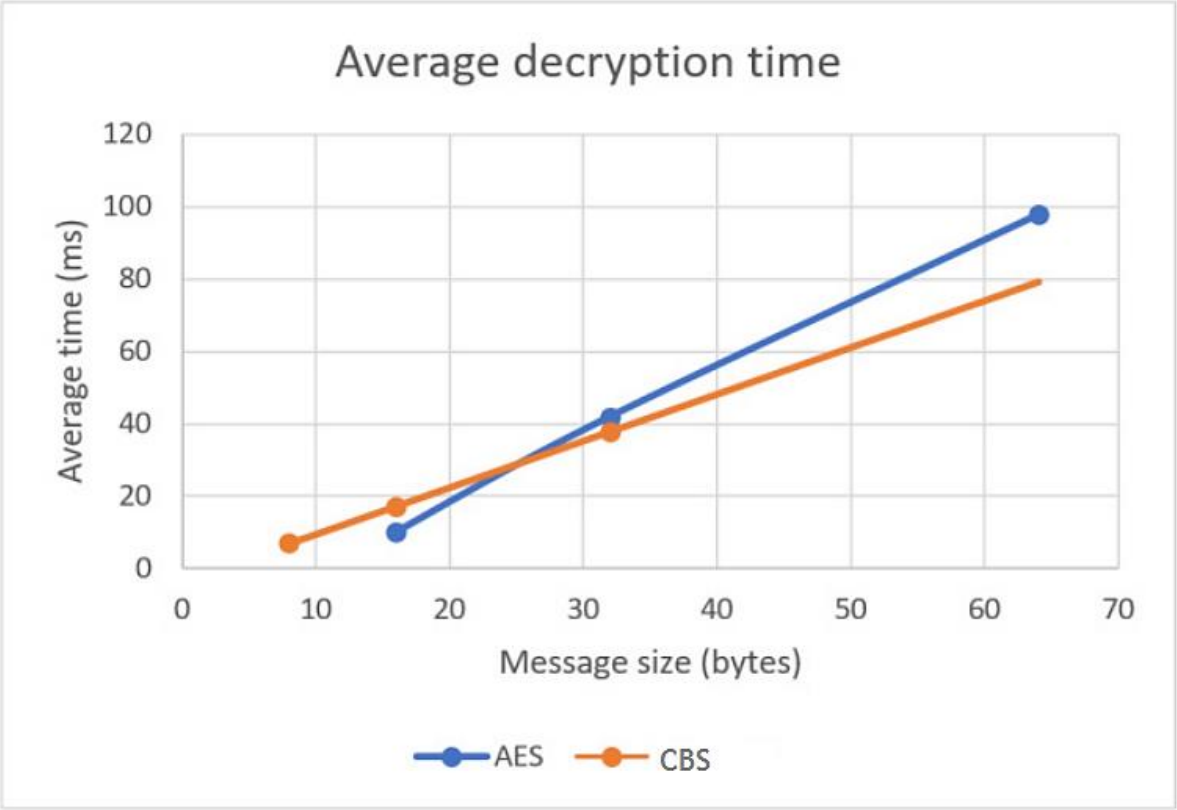


Fig. 5 - Average Decryption Time



7. Conclusion

It is crucial that our network is protected from intrusion malicious activities, encryption algorithms play an important role in achieving this objective. We need to test the algorithms with different problems like speed, throughput, reliability, etc to have an effective encryption algorithm. Because cypher block encryption is used, it is difficult to crack the attacker protection compared to the stream cypher. CBS cypher operation mode is also the most powerful because it scratches the plaintext effectively prior to each encryption. In our future work we will attempt to use other block chip encryption algorithms to optimise the sensor network security services.

References

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications magazine, 40*(8), 102-114.

Deng, J., Han, R., & Mishra, S. (2002). *INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks.* Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado at Boulder.

Karp, B., & Kung, H.T. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. *In Proceedings of the 6th annual international conference on Mobile computing and networking,* 243-254.

Papadimitratos, P., & Haas, Z. (2002). Secure routing for mobile ad hoc networks. *In Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),* (No. CONF). SCS.

Tanachaiwiwat, S., Dave, P., Bhindwale, R., & Helmy, A. (2003). Poster abstract secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks. *In Proceedings of the 1st international conference on Embedded networked sensor systems,* 324-325.

Estrin, D., R. Govindan, J. S. Heidemann, and S. Kumar. 1999. “Next Century Challenges: Scalable Coordination in Sensor Networks.” *In Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom’99),* 263-270, Seattle, Washington, USA, August 1999.

Estrin, D., Govindan, R., Heidemann, J., & Kumar, S. (1999). Next century challenges: Scalable coordination in sensor networks. *In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking,* 263-270.

Hu, L., & Evans, D. (2003). Secure aggregation for wireless networks. *In 2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings,* 384-391.

Madden, S., Franklin, M.J., Hellerstein, J.M., & Hong, W. (2002). TAG: A tiny aggregation service for ad-hoc sensor networks. *ACM SIGOPS Operating Systems Review, 36*(SI), 131-146.

Przydatek, B., Song, D., & Perrig, A. (2003). SIA: Secure information aggregation in sensor networks. *In Proceedings of the 1st international conference on Embedded networked sensor systems,* 255-265.

Shrivastava, N., Buragohain, C., Agrawal, D., & Suri, S. (2004). Medians and beyond: new aggregation techniques for sensor networks. *In Proceedings of the 2nd international conference on Embedded networked sensor systems*, 239-249.

Abd Elminaam, D.S., Abdual-Kader, H.M., & Hadhoud, M.M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *International Journal of Network Security, 10*(3), 216-222.

Sharma, K., & Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs,* 42-45.

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks, 1*(2-3), 293-315.

Stallings, W. (2005). *Cryptography and Network Security,* 4th Ed, 58-309, Prentice Hall.

Zhao, F., Guibas, L.J., & Guibas, L. (2004). *Wireless sensor networks: an information processing approach.* Morgan Kaufmann.

Schneier, B. (2008). *The Blowfish Encryption Algorithm.* http://www.schneier.comlblow -sh.html

Received: 24.06.2021 – Accepted: 24.07.2021