ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 23, December 2017

Implementation of SHA-5 Algorithm using Adaptive Channel aware detection of attacks in WSN

Ms Murugalakshmi.M(1),Mrs.A.R.Devi(2),Dr.K.Ramasamy(3)
PG Student(1),Assistant Professor of ECE(2),Principal(3)
P.S.R.Rengasamy College of Engineering for Women(1,2,3)
Sivakasi,India(1,2,3)
Email:murugaarchana@gmail.com(1),devipsrr.edu.in@gmail.com(2)

***Abstract*—Wireless Sensor Networks (WSN) is an emerging technology for attraction of researchers with its research challenges and various application domains. Today, WSN applications can be used in environmental detection, Monitoring system, medical system, military and industrial monitoring for ability to transform human life in various aspects.In existing method uses a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs.The attack tolerant data forwarding scheme can improve data delivery ratio for the network SHA5 algorithm is proposed for secure communication and to get channel aware forwarding attack detection in WSN. In proposed method use secure active detection data routing protocol (ADDRP) used to establish unique path and key .ADDRP protocol is polynomial based protocol, computation is efficient,that operates on two fixed-size blocks of data to create a hash code. This hash function forms the part of the hashing algorithm.encryption technique can be applied to transmit the data securely. This work provides an. efficient data transmit to take low energy consumption.**

***Keywords*— Secure Data Transmission, keyGeneration, ADDRP Protocol,Authentication,Data integrity,SHA 5.**

I. INTRODUCTION

The Wireless Sensor Network is built of nodes, from a few to several hundreds or even thousands, where each node is connected to one, or sometimes several, sensors.Each such sensor network node has typically several parts a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. These nodes are deployed into the environment forming a network of any desired topology. Different nodes perform different functions. Some nodes can be programmed only as sensors, some can be programmed only as carriers and some can be programmed as both. The sensing nodes send the data to the intermediate nodes. These intermediate nodes perform data aggregation or any other operation specified by the user and sends it to a Base Station (BS) receiver present at the user terminal.The WSN nodes, also referred as motes, communicate using a wireless channel. The security of wireless channel is minimal and an attacker can easily tap into the wireless stream and can view the data or modify it. To prevent these attacks,security measures are necessary to prevent unauthorised access or modification of the transmitted data [1]. Algorithms like Digital signature algorithm (DSA), RSA [2] etc, can be employed for our security necessities. However, algorithms such as DSA or RSA require large memory and processing power. A WSN mote is a very low power device and typically has an 8-bit architecture. It has very limited computational and memory resources. Hence the cryptographic algorithms to be implemented must take up a fraction of the available resources.This work employs ECDSA [3] security scheme as it is better in terms of computation speed, security and requires minimal resources. The ECDSA performs hash computation of the data and encrypts this hash using Elliptic Curve Cryptography (ECC) [4]. The hash value is encrypted using ECC point operations to obtain the Digital Signature of the data and is sent along with the data. The receiver decrypts the signature and checks for its validity. If the check fails, then the data can be sent again. In this work, SHA-512 is the hash algorithm used in the ECDSA implementation. The SHA-512 algorithm operates on 64-bit words which cannot be implemented on the mote. Hence it is modified to be compatible with the 8-bit architecture of the mote. Typical ECDSA implementations use SHA-1 as its hash algorithm. However, SHA-1 is vulnerable to attacks [5] and provides less security compared to SHA 512. This work employs SHA-512 algorithm to overcome the limitation of SHA1,SHA2,SHA3.

II. RELATED WORK

WSN's are ubiquitous computing environment and security of WSN's has quickly gained momentum in the past few years. Major focus is on the public key based security protocols.

Symmetric-key based protocols are not as versatile as the public-key system and they complicate the design of the security protocol which is not suitable to run on lower source WSN devices. Adaptive and channel aware detection of selective forwarding Attacks in WSN. Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. It high the energy consumption then security level is very low so optimal solution is poor[1]. AMD: Audit Based Mis behave Detection in Wireless Ad Hoc Networks. The AMD system integrates reputation management,trustworthy route discovery. No awareness about energy of the node[2]. A Survey of Intrusion Detection Systems in Wireless Sensor Networks Intrusion Detection Systems (IDSs) that are proposed for WSNs. Selfish node don’t find accurately detection of any attack [3]. Enabling Trust worthy ServiceEvaluation in Service-Oriented Mobile Social Network Trustworthy Service Evaluation (TSE) and service-oriented mobile social networks (S-MSNs) No awareness of attacker [4]. Exploiting Channel-Aware Reputation System Against Selective Forwarding Attacks in WSNs Channel aware Reputation System (CRS) to identify. It does not low energy consumption and delay is high [5]. SACRM: Social Aware Crowd sourcing with Reputation Management in Mobile Sensing Social Aware Crowd sourcing with Reputation Management It does not improve network life time in the effect on the noisy channels[6]. Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks link-disjoint paths from all available paths. A congestion control and load-balancing algorithm that can adaptively. It does not Hop-by-Hop Authentication is available. [7] proposed a novel method for secure transportation of railway systems has been proposed in this project. In existing methods, most of the methods are manual resulting in a lot of human errors. This project proposes a system which can be controlled automatically without any outside help. This project has a model concerning two train sections and a gate section. The railway sections are used to show the movement of trains and a gate section is used to show the happenings in the railway crossings. The scope of this project is to monitor the train sections to prevent collisions between two trains or between humans and trains and to avoid accidents in the railway crossings. Also an additional approach towards effective power utilization has been discussed. Five topics are discussed in this project : 1) Detection of obstacles in front of the train;2) Detection of cracks and movements in the tracks;3) Detection of human presence inside the train and controlling the electrical devices accordingly 4) Updating the location of train and sharing it with other trains automatically 5) Controlling the gate section during railway crossing. This project can be used to avoid accidents in the railway tracks.Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks. Propose the user scheduling scheme to achieve multiuser diversity. It does not improve convergence speed and also delay occurring[8]. EAACKA Secure Intrusion-Detection

System for MANETs. Enhanced Adaptive Acknowledgment (EAACK) specially designed for

MANETs. CH selection is computationally expensive task[9]. Distribute anomaly detection for industrial wireless sensor networks based on fuzzy data modelling. *fuzzy c-means* clustering in an incremental scheme. It does not give accurate result[10]. A novel scheme for WSAN sink mobility based on clustering and setpacking technique. Clustering and set packing Technique. The sensors alone are unable to control the sink and need to send or relay a smaller amount of packet data. It does not Mobility concept needs more maintenance[11]. Mitigatig Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenge. The Optimized Link State Routing protocol (OLSR) is a proactive routing protocol designed for large networks. the use of MPRs which are a set of neighbor nodes that represen**t** the unique responsible for spreading the local link state information. No improve convergence speed and also no computation cost reduces[12]. Data security in unattened wireless sensor networks. We focus on unattended WSNs (UWSNs) characterized by intermittent sink presence and operation in hostile settings. It does not Maintenance of the network[13].

III. SHA5 ALGORITHM

1) SHA-512 Algorithm: SHA stands for Secure Hash Algorithm. There are many variants of SHA i.e. SHA-0, SHA-1,SHA-2 and SHA-3. Each variant is a set of hash functions. The SHA-512 algorithm is classified under SHA-2 which is a setof cryptographic hash functions designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. federal standard (FIPS). The SHA-512 algorithm has a maximum message size of 2128 bits and operates on a 1024-bit blocks. It has 80 rounds of processing and operates on 64-bit word data. It produces an output message digest having a size of 512 bits. Each 1024-bit block is processed to produce a 512-bit hash which is added to the previous hash. This aggregation of the hash values of each 1024-bit block gives the final hash value of the entire message. The security of a hash function is directly related toits message digest length [20]. SHA-512 has a message digest length of 512 bits which is significantly higher than SHA-1. This clearly makes the SHA-512 algorithm better than SHA-1 in terms of security. Table I gives the specifications of SHA-512 which shows that the security of SHA-512 is greater than any of its predecessors.

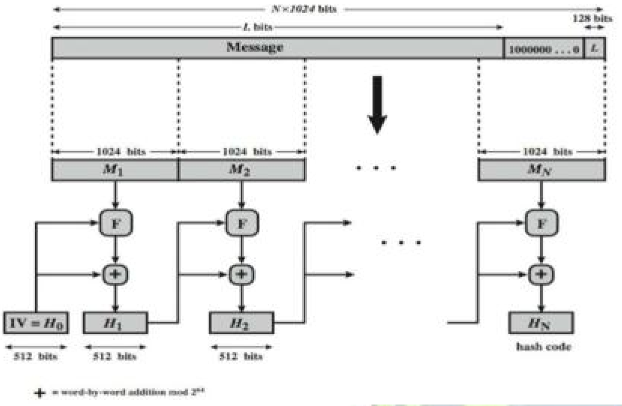

Fig 1: SHA 5 Encryption process of 1024-bit blocks single round

SHA 5 ALGORITHM STEPS :

Step 1 : Appending padding bits

Step 2 : Append Length

Step 3 : Initialize hash buffer.

Step 4 : Process the message in 1024bits (128words) blocks which forms the heart of the Algorithm.

Step 5 : Output the final state value as the resulting Hash.

Hash formula:

$$h=H(M)$$

h-hash function of fixed length

M-message length

H(M)- hash function of different length

Sample encryption and decryption process

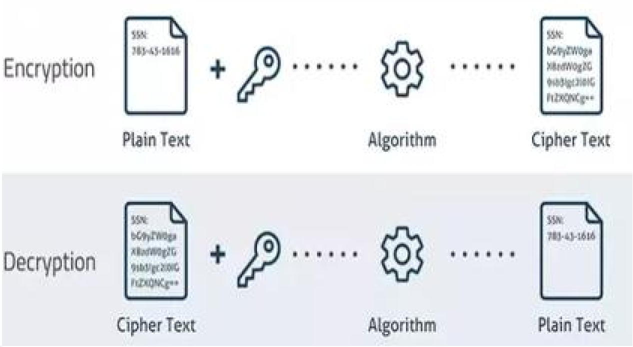

Fig 2:Encryption and Decryption process

IV. METHODOLOGY

1) Creating Network Formation

2) Neighbor discovery

3) Algorithm implementation

4) ADDRP protocol implementation

5)misbehaviour detection

6)performance analysis

CREATINGNETWORK FORMATION:

In our simulations, the network area is 1200m*300m with 60 nodes initially and uniformly distributed .The channel capacity is 2mpbs.The Transmission range is 150m.A total UDP based CBR sessions are used to generate the network traffic. For each session, the data packet are generated with the size of 512 bytes in the rate of 16kpbs.The source –destination pairs are chose randomly from all nodes. The simulation work has been done with the Network Simulator ns-2, Version 2.34. Network formation is an aspect of creating nodes of network and transmit data. Network of 100 nodes is created using network simulator for wireless sensor network

NEIGHBOUR DISCOVERY:

When a source node needs to find a route to a destination, it starts a route discovery process, based on flooding, to locate the destination node. Upon receiving a route request (RREQ) packet, intermediate nodes update their routing tables for a reverse route to the source. Route request send to all intermediate nodes between source and destination. Route discovery for shortest and freshest path.After reaches the destination node- Sends Route reply packets to source node.Transmit the data from source node to destination node through energy efficient intermediate nodes, If any path failure occurs again starts route discovery.

ALGORITHM IMPLEMENTATION:

Encryption decryption is done by SHA5 Algorithm.Detection of misbehavior nodes using Security Packet, then send communication between source to destination node.SHA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. If the authentication is successful then it sends data packet through the Reliable routing path.SHA5 provides end-to-end confidentiality and hop-by-hop authentication.

ADDRP IMPLEMENTATION:

Secure active detection data routing protocol (ADDRP) used to establish unique path and key ADDRP protocol is polynomial based protocol,computation is efficient .Active detection route to identify the black hole attack and mark the blacklocation. It avoid the black hole attackers through the active creation number of detection routes. Detection route increase the lifetime and improve the data route security. we use in black hole attack are identify the filtering packets from attack source single malicious node cause thousand of node become disconnected and other node eliminate such attacks.

MISBEHAVIOUR DETECTION:

Route request send to all intermediate nodes between source S and destination D. Route discovery for shortest and freshest path using ADDRP. Check the Neighbor list.Detection of misbehavior nodes using Security Packet.Then send communication between source to destination node.we use selective forwarding attack can be classified in two way, one is Active black hole another passive attack. Active black hole attack: Node receives the RREQ packet and returns false RREP packet.

PROPOSED WORK:

In this paper, we can propose private key Cryptography Technique that helps to reduce the network overhead.The count of acknowledged packet increases when the number of malicious node in network increases due to this reason, network overhead increases. Therefore, to reduce the network overhead we can use private key Cryptography Technique. secure active detection data routing protocol (ADDRP) used to establish unique path and key ADDRP protocol is polynomial based protocol, computation is efficient .Active detection route to identify the selective forwarding attack and mark the black location. It avoid the black hole attackers through the active creation number of detection routes. Detection the data route security. we use in black hole attack are identify the filtering packets from attack source single malicious node cause thousand of node become disconnected and other node eliminate such attacks.

SYSTEM ARCHITECTURE:

The Proposed system uses the technique of SHA5 due to which private key Cryptography scheme provides three cryptography primitives called as Integrity,Confidentiality and Authentication. A key exchange mechanism eliminating the requirement of predistributedkey,which examine the possibilities of adopting. For providing security encryption mechanism and SHA5 key exchange mechanism is to be considered. To perform encryption and decryption technique each node must have approach to other nodes key. At origin, neighborhood key is encrypted with the public key of the receiver and transmitted to the terminal node. At terminal neighborhood key is decrypted with the node’s own private key. The message specific key is having the advantage of making it to improve the security of the message being forwarded in the wireless sensor network. .

V . PERFORMANCE EVALUATION:

Simulation Configuration:
Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with ubuntu. The system running with 3-GBRAM. In order to better compare our simulation. In NS2.34, the default configuration specifies 50 nodes in a flat space with size of 670×670m.The language we are using are TCL and AWK script. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 521B. In order to measure and compare the performance of our propone scheme, we adopt the following performance.

- **Packet delivery ratio**
- **Throughput**
- **Delay**
- **Transmission range**
- **Packet drop**

- **Network lifetime**
- **Energy consumption**

PDR GRAPH:

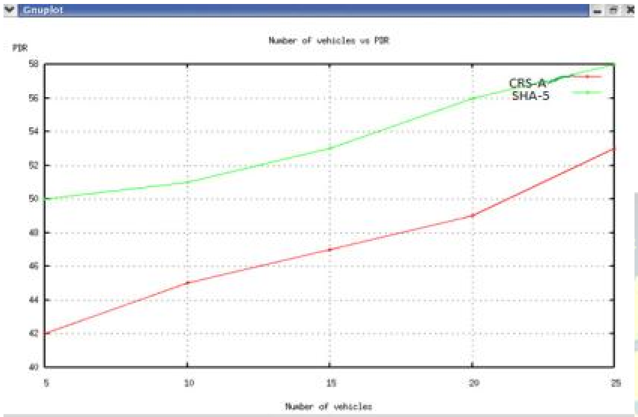

Fig :Packet delivery ratio

THROUGHPUT GRAPH:

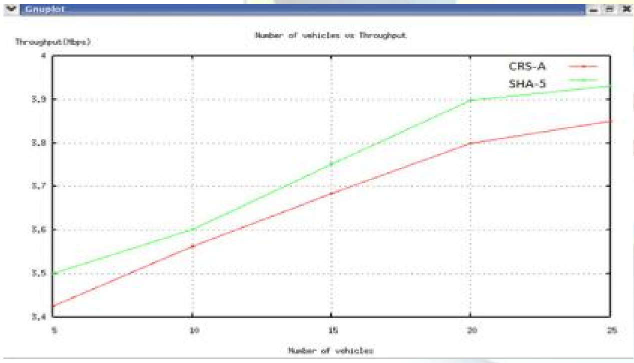

Fig:Throughput

DELAY GRAPH:

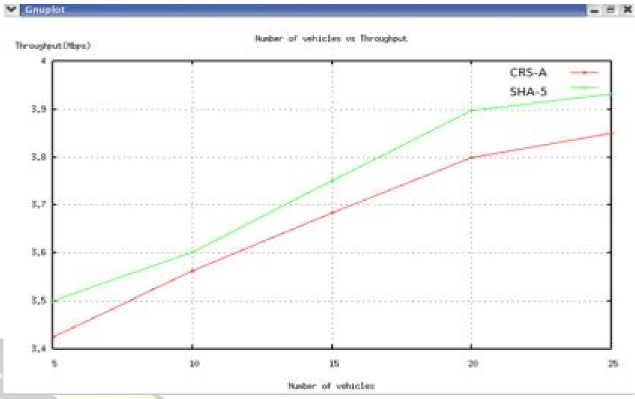

Fig :Delay

TRANSMISSION RANGE GRAPH:

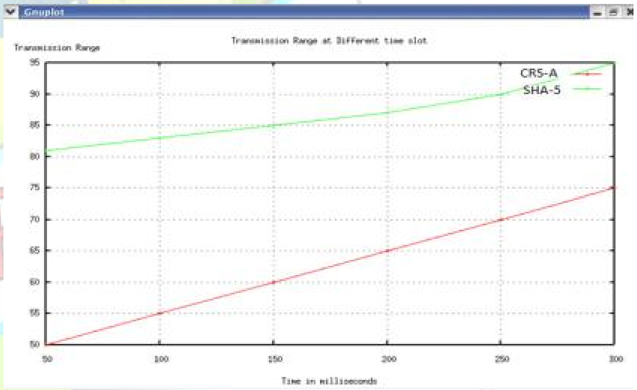

Fig :Transmission range

PACKET DROP GRAPH :

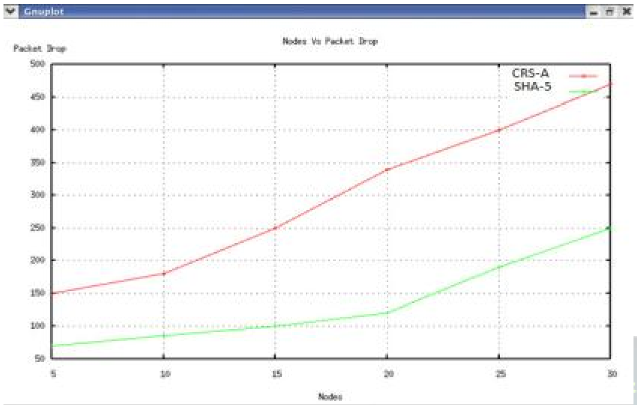

Fig :Packet drop

NETWORK LIFE TIME GRAPH:

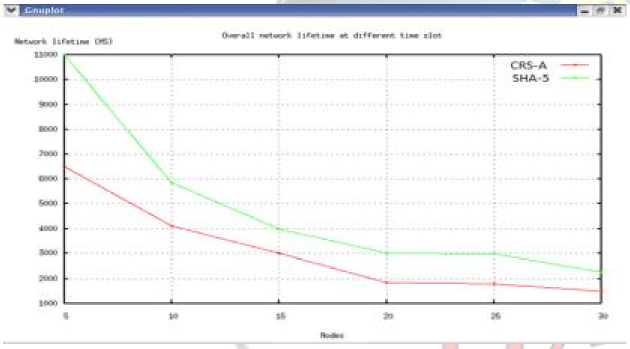

Fig:Network lifetime

ENERGY CONSUMPTION:

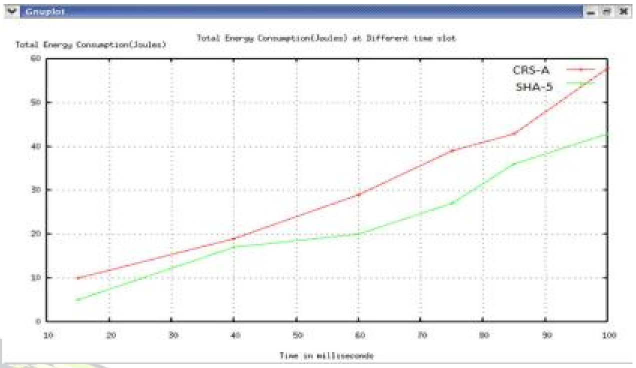

Fig:Energy Consumption

CONCLUSION

In these paper we have purpose the terminologies in security of WSN using method are concentrating only detection of malicious nodes we use private key cryptography used in encryption to strengthen the security of nodes. Detection of malicious node can be done by ADDRP using RSA algorithm. To improve security. As further analysis, more security and authentication agent into NS-2 using hashing algorithms such as SHA-256, SHA-384, SHA- 512 for encryption /decryption. With this approach researchers can also add his or her own combined security and integrity Agent into NS-2 by introducing new encryption/decryption and hash functions.

REFERENCES

[1] Ju Ren, student member, yaoxue zhang,kuan zhang, and xuemin shen," Adaptive and channel aware detection of selective forwarding Attacks in WSN," IEEE transaction of wireless communications,vol xx,no.xx, xxx 2016
[2] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., Sep. 2016, doi: 10.1109/TMC.2012.257, to be published.
[3] I . Butun, S. Morgera, and R . Sankar, "A survey of intrusion detection systems in wireless sensor networks,"IEEE Commun. Surveys Truts. , vol. 16, no. 1, pp. 266–282, May 2014
[4] X. L iang, X. Lin, and X. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," IEEE Trans. Parallel Distrib. Syst. , vol. 25, no. 2, pp. 310–320, Feb. 2014
[5] J. R en, Y. Zhang, K. Zhang, and X. Shen, "SACRM: Social aware crowdsourcing with reputation management in mobile sensing," Comput.Commun. , vol. 65, no. 15, pp. 55–65, 2013
.[6] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," IEEE Trans. Commun., vol. 61, no. 12, pp. 5103–5113, Dec. 2013.
[7] Christo Ananth, K.Nagarajan, Vinod Kumar.V., "A SMART APPROACH FOR SECURE CONTROL OF RAILWAY TRANSPORTATION

SYSTEMS", International Journal of Pure and Applied Mathematics, Volume 117, Issue 15, 2017, (1215-1221).

[8] H.Kumarage,I. Khalil, Z.Tari, and A.Zomaya," Distribute anomaly detection for industrial wireless sensor networks based on fuzzy data modelling," IEEE transaction on industrial informatics 2013.

[9] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in wmns," IEEE Trans. Wireless Commun.,vol. 9, no. 5, pp. 1661–1675, 2010.

[10] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," Comput. Commun., vol. 31,no. 17, pp. 3941–3953, 2008.

[11] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify suspect nodes in selective forwarding attacks," J. Parallel Distributed Comput., vol. 67, no. 11, pp.1218–1230, 2007.

[12]K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing Misbehavior in manets," IEEE Trans. Mob. Comput., vol. 6, no. 5, pp 536–550, 2007.

[13] R. Shaikh, H. Jameel, B. d'Auriol, H. Lee, S. Lee, and Y.-J. Song,"Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distr. Sys., vol. 20, no. 11, pp. 1698–1712, 2009.

[15] L. J. Chen, Z. Y. Shan, T. Tang, et al., "Performance analysis and verification of safety communication protocol in train control system", Computer Standards & Interfaces, Vol. 33 Issue 5 pp. 505-518, 2011.

[16] L. Dai and K. Cooper, "Modeling and performance analysis for security aspects", 4th International Workshop on Systems/Software Architectures, Las Vegas, USA, 2005, Science of Computer Programming, Vol. 61 Issue 1, pp. 5871, 2006.

[17] W. Nowakowski, "Information security and privacy protection in emergency management software systems", Logistyka 4/2015, str. 8072-8077, 2015.

[18] O. B. Montoya Alber, A. G. Munoz Mario and T. Kofuji Sergio,"Performance Analysis of Encryption Algorithms on Mobile Devices",47th International Carnahan Conference on Security Technology (ICCST), Medellin, Colombia, 2013.

[19] S. Ji, T. Chen and S. Zhong, "Wormhole Attack Detection Algorithms in Wireless Network Coding Systems", IEEE Transactions on Mobile Computing, Vol. 14 Issue 3, pp. 660-674, 2015.

[20] EN 50159, "Railway applications - Communication, signalling and processing systems - Safety -related communication in transmission systems", 2010.

[21] Z. Łukasik, W. Nowakowski W, "Wymiana informacji w systemach związanych z bezpieczeństwem", Logistyka 6/2008.The International Conference on Information and Digital Technologies 2017978-