IJCSN -International Journal of Computer Science and Network, Volume 7, Issue 6, December 2018
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Energy Conservation and Data Secure Communication in Wireless Sensor Network

Gaudence Stanslaus

School of Telecommunication Engineering, Xidian University,
Xi'an 71007, China.

Abstract – In wireless sensor network, the process of sensed data information based on the network location, converting and transmitting to base station consume energy and need security, maintain network lifetime is main issues. The article present methods, which used to sustain energy lifetime of the sensor node and secure data transmission within the wireless sensor network. The digital watermark and routing algorithm used to ensure safety transmission for packet and maintain energy consumption for sensor node. The greedy perimeter packet stateless routing indicates that the processing data packet for network size of 300 and 400 unnumbered nodes use only 16.4925% compared with present invention method which consume 83.5075% with the same network size. The simulation results indicate greedy perimeter packet stateless routing is less processing power and it uses less time processing compared to other methods through experimental.
Paper also, present review about techniques methods, which used to reduce energy consumption and energy harvesting within WSNs.

Keywords - *wireless sensor network, digital watermarking, network lifetime, energy lifetime, energy consumption.*

1. Introduction

Wireless Sensor network (WSN) sometimes-called sensor network are spatially distributed network sovereign sensor to monitor physical or environmental condition such as temperature, sound, pressure etc [1]. The WSNs built of numbers sensor nodes from a few to several hundreds or thousands and each node connected to one or sometimes several sensors. All connected sensors has several part used for communication such as radio receiver with internal antenna or connected to external antenna, a microcontroller as an electronic circuit for interfacing with the sensors and an energy source. The WSN deployed in most dangerous region that people could not get there easily such as mining, underwater, forest, battlefield and other destructive areas. The WSN contains sensor nodes, which communicate over the short distance via a wireless communication medium [2].

The development of WSN motivated by military application such as battlefield surveillance [3]. Nowadays WSN is a worldly new technology to electronic devices for several industrial applications such as, monitoring and control devices, machine health monitoring, air and water quality management, homeland security monitoring and smart home system, habitat monitoring, hazard monitoring i.e. chemical weapon, disaster monitoring i.e. forest fire or flash floods, gates control, motion and shock detector [2], [4].

There also an increase application for which the WSN may be utilized such as wildlife monitoring [5], [6], [7] mapping environmental [8], [9] and traffic monitoring in a smart city [10], [11]. Not only that but also, application in emergency scenario such as monitoring vital signs [12], [13], [14] in temporary hospital and the use of unmanned aerial vehicles (UAVs) in the aiding of search and rescue (SAR) [15], [16].

Regarding all the applications but the WSNs is a low cost maintenance network with reliable data collection and low energy consumptions [2], [6]. The sensor nodes, which used to connect the WSN consists of the very small tiny sensors nodes with limited resources such as lower batteries for power , memory capacity and the processing system. The function of sensor nodes is to sense the environmental condition based on its location and its target and send to base station (BS).

The WSNs delivers maximum respond to all types of electronics industry nowadays. The establishment of the internet technology like Internet of Things (IoT) which enhance the WSNs as apart to ensure all devices are connected together and enabling them to send and receive data. The embedded system and the application of the WSN has a greatly contribution to the world industrial development.

The communication of sensor nodes both for sending and receiving packets within a network from one node to another have many challenges as comparing with traditional network like wireless local area

network (WLAN) or local area network (LAN) protocol when consider security mechanism [17]. Thus, packets over WSNs are vulnerable to internal and external attacks.

Relating with traditional networks aforementioned, the WSNs contains many difference insights regarding data packets securities within the network. The major difficult for WSNs is the network operational. The difficult part may involves in the network setup and the security configuration from sensor nodes to the BS.

Most security in typical network include confidentiality, routing security, bad behavior detection of nodes and other vulnerability about the data. Considering the existing traditional network, there is clear arrangements of nodes through the network setup, there are the end system like servers and nodes, intermediate systems like hub, routers, switches, bridges and repeaters, but in WSNs, each node is potentially a router or a switch by itself for some other node within the network connectivity.

It is difficult to employ the existing securities like symmetric cryptograph for encryption and decryption for the purpose of data confidentiality, authentication, availability and integrity approaches to WSN [18]. The symmetric key algorithm has disadvantages of key distribution that requires more memory size and asymmetric key algorithm need much computation process that requires more power [18]. As depicted early sensor node contains a few memory size kilobytes (kb) and limited amount of power processing. The existing securities system mentioned will cause batteries exhaust, sensor nodes may fail on its application, and the whole network will be down.

The routing in WSN is key important task that is to be carefully handling for case of data communication. Routing techniques needed for sending data from the sensor nodes to BS.

The contributions of this paper are as follows;

a) The application of using routing algorithm decrease network lifetime and ensure batteries are not exhaust and sensor node failed or blocked in its application.
b) To ensure network attackers are not tempered with data packets transmitted by the sensor nodes through the network
c) Introduce the methods for energy lifetime conservation efficiency techniques in WSN
d) The article ensures every aspect of the WSNs application would collect or disseminating the sensitive information from the network using the watermark design technology.

Due to the requirements of the application of the sensor node in the WSNs, the main issue to address is a way to reduce the energy consumption so that it will extend the batteries lifetime of the sensor nodes. Ordinarily batteries in each sensor node are equally during the network setup. When networks starting transmission and processing data the energy of sensor node will differ from one node to another. These is due to each sensor node responsibility based on the network setup like location and size of the network.

In this particular some nodes cannot used as routing nodes and the network routing performance will be failure. Some researcher suggests many design protocols to adapt to the variety of the application [11]. The application provided for this routing algorithm are reactive, proactive and geographical location [19].

Amongst the routing protocol for forwarding packet from one node to another is greedy perimeter packet stateless routing (GPSR) [19]. A geographical routing protocol provide efficiency self-organized ad hoc network. The GPSR is the protocol that is suitable to geographical location for some reasons [20]. In geographic routing, the nodes require only location information of their direct neighbors or next node in order to forward the packets and hence use less memory space.

In order to extend the services of the network, we consider the energy for the sensor node. In GPSR algorithm when sensor node chooses routing path it only needs to know the geography, location of itself, the neighbor node, and the target nodes.

The GPSR consists of two methods for forwarding packets among sensor nodes in sensor network. The greed transmission that used wherever possible, and border transmission that used in the region greed transmission [19]. The main characteristic of the energy aware routing protocols that the aim to maintain a global balance of residual energy in each node in order to delay excessive lifetime of the entire network. Attoungble [20] and Kong [21] propose the geographic energy aware routing (GEAR) that extend network lifetime by involving several neighbors in the data packet forward process. However, their method of forwarding packet creates another new problem to WSN that they use all the neighbors in the packet forwarding, which requires nodes to use paths that are not necessary energy efficient, which requires long paths.

The greedy algorithm with geographical area in WSNs may fails at voids node [22]. The face routing meets the network graph and forward a message along one or a sequence of adjacent faces, which provides progress towards the sink node.

In this article, the author proposes a secure communication, efficiency energy consumption and security within the WSNs. The proposed system

involves the application of the watermarking techniques, routing algorithm using the GPSR.

The watermark techniques hiding digital information in the source node packet to the carrier transmission. The watermark consists of two parts; code embed where it hiding digital information and code decode as the decoding to compare the origin of data.

The source node forward the packets after finding the next neighbor node which using the algorithm for forwarding the packets received from the source node to sink node which determine the watermarks by compare if data are tempered or not tempered. Upon the reception of the data, the Sink node can be able to authenticate data by validating the watermarks, thereby detecting whether the data illegitimately altered. In this process, the aggregation survivable authentication information added at the sources node and checked by the sink node without any involvement of intermediate node as shown on Fig.1.

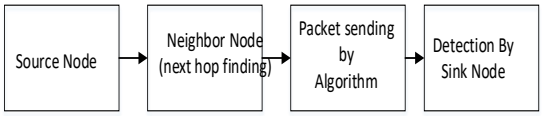

Fig.1: Data movement from source sensor node to sink sensor node

2. Related Works

2.1 Watermarking Techniques in wireless Sensor Network

The techniques of watermarking are the process, which allows an individual to embedding the information into to data packet for the case of hiding copyright of the data packet which transmitting to WSNs. The watermarking techniques consists of three main steps [23], [24];

a) Watermarking generation process

This is the first step in the watermark system, and very critical one. The requirements of the watermark generation process are unique, complex. The message contains on the watermark, and key must be unique for the reason of make a secret code for transmission. The key embedding and watermark information produced in watermark generator to produce watermark signal.

b) Watermarking embedding process;

This process undertaken by embedder and can be done in the transmission domain. The embedder combines the cover medium, the watermark signals, the sensed data and the key embedding and creates the watermarked cover medium.

The embedder combines the cover medium of the watermark signal and sensed data together with the key embedding to create a watermark cover medium.

c) Watermarking detection and extraction process.

This is the third process for the watermark system and it is a crucial part as it enables the sender to identify and provide information to the intended receiver. Detector undertakes the process of extraction or detection [25]. The detecting process consists of extraction units to first extract the watermark signal from the watermark cover medium, and then compare it with the original watermark signal from the cover medium.

During transmission of data packet from the generation process in the source node, to the detection and extraction in the sink node, there are many interferences within the transmission. Those interferences caused the noise and decrease the quality of transmission and leading the watermarked cover medium being dropped and be susceptible to attacks as shown Fig.2.

In this model, watermark information is generating and embedded at the source sensor nodes. The extraction and verification of the copyright at the sink sensor nodes side and risk of data packets are at the transmission channel. The aim of those attacks is to remove watermark signals from the cover medium.

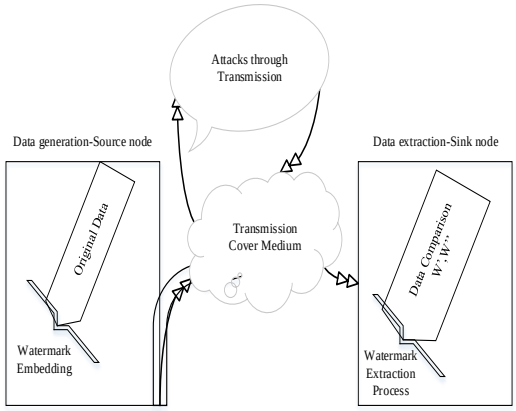

Fig.2: watermark detection and extraction Model

2.2. Energy Efficient Techniques for Wireless Sensor Network

Through the energy, harvesting and energy consumption techniques for the WSNs there are factors, which identify the energy efficient techniques for the WSNs. Those factors elaborated in classes as duty cycling, data

reduction, protocol overhead reduction, energy efficient routing, and topology control [26].

a) Data reduction: focuses on reducing the amount of data produced, processed and transmitted. For instance, data compression and data aggregation are examples of such techniques
b) Protocol overhead reduction: the aim of this technique is to increase protocol efficiency by reducing the overhead. Transmission periods of messages are adapted depending on the stability of the network, or on the distance to the source of the transmitted information. More generally, a cross-layering approach will enable an optimization of the communication protocols taking into account the application requirements.
c) Energy efficient routing: routing protocols designed with the target of maximizing network lifetime by minimizing the energy consumed by the end-to-end transmission and avoiding nodes with low residual energy. Byamukama at el [27] suggest how to reduce the power consumption of gateways in WSNs deployed in environment monitoring applications, such as Automatic Weather Stations (AWS). Power failures reduce the availability of the network and cause both hardware failures and software corruption. These can add operational costs for repair or replacements [28] and increase the requirement for local technical.
d) Duty cycling: duty cycling means the fraction of time nodes are active during their lifetime. Nodes sleep/active schedules should be coordinated and accommodated to specific applications requirements. Anastasi at el [29] propose, some of the sensor nodes are mobile, mobility could be used as a tool for reducing energy consumption.
e) Topology control: it focuses on reducing energy consumption by adjusting transmission power while maintaining network connectivity. A new reduced topology created based on local information. Bandyopadhyay and Coyle [30] propose the distributed, randomized clustering algorithm to organize the sensors in a wireless sensor.

3. Proposed Digital Watermark Methods

The watermarking technique provide reliability of copyright of data packet protection. By using the digital watermark, techniques to ensure the data packets are safety through the transmission process in the WSN. Methods and steps used in algorithm for watermark are as follows;

1) Method 1: Within the network, the watermark generated and embedded data packet for transmission. The optimal evaluation must be consider for the next hop based on the distance for the purpose of the security and energy consumption. Each packet carries 8 bits which is int32 types of data, and number for each int32 are 0,1,2,3,4,5,6,7.The redundant space or shifted data is 4 $bits$, and an embedder code number will be low in is 4 $bits$ for each 32 data sequence. As indicates Fig.3 shifted data space is$R(i) = \{r_0, r_1, r_n\}$, where n represent data field, r represents the size of the shifted data of i^{th} data field. During transmission, the data field converted to binary sequence number.

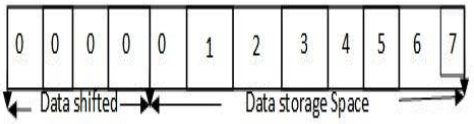

Fig.3; Data Embedding Process for shifted data field

2) Method 2: Within the network for the receiving side; the data packet with the shifted data as watermark code in the sink node, it will judge whether the data packet tampered or not during transmission process from source node to destination sink node. We extract the low 4 $bits$ of each int32 data as follows; if the low 4 $bits$ can form a series sequence; 0,1,2,3,4,5,6,7 then we determine this data packet is secure. Unless if the low 4 $bits$ cannot form series sequence likewise, may be like this; 0,7,1,3,5,6,2,4 or any other form, then we determine the data carried by this packet is insecure, and possible were tampered with an attacks during the transmission within the network. In Fig.4, the watermark extraction process shows that data have been convert to binary system and comparing from data sent from source to the receiving side on the sink node.

The steps used for data source preparation as encryption process, transmission process and receiving data or data description process for the watermark in WSNs are as follows:

1) Step one; sensor node setup in WSNs; the arrangements of connectivity of WSN includes the source node, sink node and an

intermediate node$B = \{B_1, B_2, L, .. B_n\}$. The source node (N) is responsible for generating the watermark packet and destination $Sink$ node is for receiving the data packet while the intermediate node $B = \{B_1, B_2, L, .. B_n\}$ that consists of energy , location and security is responsible for transmitting the watermark packets generated by source node N to the destination $Sink$ node.The intermediate node denoted as energy $E_I \epsilon [0,0.2]$, security as $S_I \epsilon [0, 10]$ and for the location denoted as $[X_i, Y_i]$ respectively.

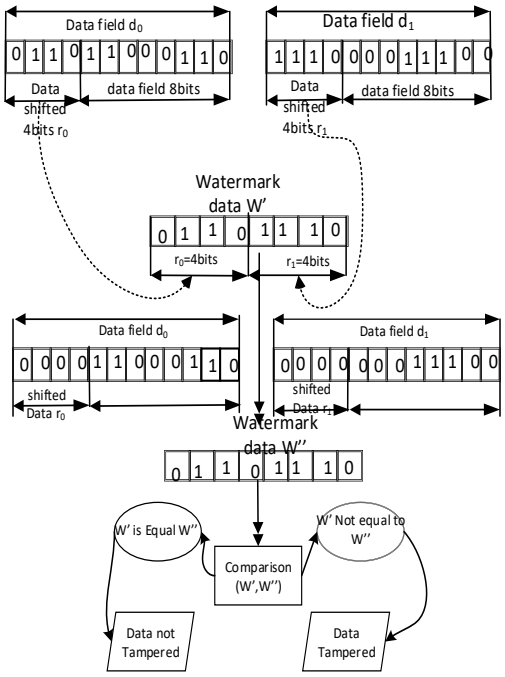

Fig.4; Data packet received extraction process

2) Step two; The process of generate the watermark Packet in Source node;
   a) The watermark packet generated in source node N and the original packet is $[data = \{data_1, data_2, L, data_i, L, data_8\}]$ where the first i data item $data_i$ consists of 28 $bits$ binary sequence $i = 0,1,,2, \dots 7$.
   b) Source node N generates a 32 $bit\ raw$ watermark sequence $w = \{w_1, w_2, L, w_i, w_8\}$ where the first watermark consists of 4 bit binary sequence $i = 0,1,2, \dots 7$.
   c) By adding, the first watermark to the first data item obtaining the 32 $bits$ first watermark data item and it keeps on repeat the process until a watermark packet received $wdata = \{wdata_1, wdata_2, L, wdata_i, L, wdata_8\}$, $i = 0,1,2, \dots 7$ as shown Fig.5.

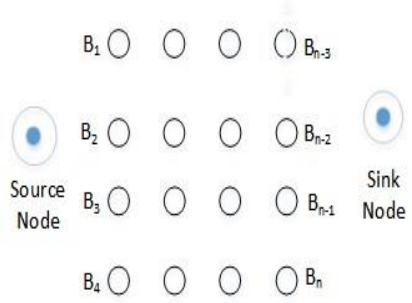

Fig.5; Sensor Node Network connection

3) Step three; The process of Select the neighbor Node within the network
   a) Select the source node N as the current node, based on the U
   b) The distance from the current node to the destination node can be formulated from the ideal Euclidean metric [31] refer Eq. (1).

$$d_{usink} = \sqrt{(X_u - X_{sink})^2 + (Y_u - Y_{sink})^2} \quad (1)$$

Thus, (X_u, Y_u) is the location of the current node and (X_{sink}, Y_{sink}) is the location to the destination node $sink$ node.

   c) The area of the circle from the source node to destination node using the formula [32], as shown Eq. (2).

$$TR = \pi R^2 \quad (2)$$

Where, TR is the transmission range and π is given $pi = 3.14$, R is the radius from the current node$U$, to find current node N of the transmissionTR, all the intermediate nodes within the candidates neighbor node, to get the neighbor node set $B^m = \{B_1^m, B_2^m, L, B_i^m, L, B_m^m\}$.

   d) By refer the distance between two points as refer on 3b above the distance formula, we calculate the first i candidate neighbor node B_i^m to the distance node $sink$ and

distance d_i with the current node U to the distance node $sink$ distance from d_{usink} as indicated Eq.(3).

$$d_i = \sqrt{(X_i - X_{sink})^2 + (Y_i - Y_{sink})^2} \quad (3)$$

In case $d_i < d_{usink}$ then the first i neighbor node B_i^mas a neighbor node into the neighbor node collection B^H inside among (X_i, Y_i) as a candidate neighbor node B_i^m position $i = 1,2,3,..m,(X_{sink}, Y_{sink})$ as a destination to the sink node position.

e) The process will be repeating on step 3(d) until the candidate neighbor node set is processed to $B^H=\{B_1^H, B_2^H, L, B_i^H, L, B_h^H\}$

4) Step four; forwarding the watermark packet;

a) According to the formula, $m_i = \frac{\alpha D_i}{\beta E_i + \gamma S_i}$ we calculate the first neighbor node B_i^H of the quality assessment. Among the D_i said the first i neighbor node B_i^H to the destination node $sink$ distance E_i said to be the first *i* neighbors.Node B_i^H is the energy of S_i said the first i neighbor node B_i^H the degree of the security $i = 1,2,....h$ and α, γ and β are constant, the range [0,10].

b) The steps keep on repeating 4(a) until the neighbor node set calculated to $B^H = \{B_1^H, B_2^H, L, B_i^H, L, B_h^H\}$ the quality of all nodes in the evaluation is$m = \{m_1, m_2, L, m_i, m_h\}$.

c) The quality assessment $m = \{m_1, m_2, L, m_i, m_h\}$ sort the neighbor node with the lowest quality assessment selected as next hope node, receive by the current node U forwarding the watermark packets $wdata$ and records the next hope node to the data-forwarding node set C inside.

d) The next hope node as the current node U, then repeats steps 3(b) through 4(c) until the watermark packets are attached $wdata$ sent to the destination node $sink$, get the received data packet $rdata = \{rdata_1, rdata_2, L, rdata_i, L, rdata_8\}$ and a collection of data packet forwarding nodes $C = \{C_1, C_2, L, C_i, L, C_r\}$

5) Step five ; watermark extraction and detection

a) The destination node $Sink$ followed by receiving packets from $rdata = \{rdata_1, rdata_2, L, rdata_i, L, rdata_8\}$ In the interception of the first i data item$rdata_i$ the last four, a $32\ bits$ received watermark sequence is obtained $rw = \{rw_0, rw_1, ...rw_7\}$ where the first i receive watermark items rw_i Consisting of a $4\ bit$ binary sequence, $i = 0,1,2,\cdots 7$.

b) According to the formula, the received watermark sequence $rw = \{rw_1, rw_2, \mathrm{L}, rw_i, \mathrm{L}, rw_8\}$ with the original watermark sequence $w = \{w_1, w_2, \mathrm{L}\ w_i, \mathrm{L}, w_8\}$ is the error, among them $\oplus$ said XOR operation, $err = rw \oplus w$.

c) If the err equal to0, that indicates that the packet is received correctly. Contrary, if err not equal to 0 , indicates that the packet has been tampered with, according to the formula ,the data collection node set obtained by step (4d) is modified in turn $C = \{C_1, C_2, \mathrm{L}, C_i, \mathrm{L}, C_r\}$ in each node of the security,

$$S_I' = \begin{cases} \frac{S_i}{2} & err \neq 0 \\ S_i & err = 0 \end{cases} \quad (4)$$

Among S_i versus S_i' respectively i data forwarding node $C_i$the current safety and the modified safety.

6) Step six; repeat steps two through step five, until any intermediate node in the wireless sensor network cannot find the next hop node that satisfies the condition to terminate when the packet is forward.

4. Simulation Results

4.2. Energy conservation lifetime setup experiment

The specific process of the network lifetime experiment of the invention are first from the source node sensor denoted as N after generating the original data packet, the watermark codes inserted to get the watermark packet, and then through the routing algorithm we calculate the next hop node for packet forwarding. Finally, the watermarks packet sent to the destination node. In an experiment, source node N continue to generate watermark packets, until any intermediate node in the WSN failed to find the next hop node that satisfies the condition to terminate when the packet is forwarded.

The invention uses the network lifetime as the basis for testing the performance of the GPSR method and network lifetime defined as the duration of a packet in a WSN that can continuously send packets. Apparently, the longer the network life for the data processing, the more energy consumed in the nodes of the network and the shorter the network lifetime for data processing, the less the energy usage of the nodes in that network.

The parameters of the method of present invention ES for α, β, γ are $2, 4.5, 0.1$ respectively. In addition, the node transmission radius R equal to$70m$, the initial energy of the intermediate node is 0.2 watts, the intermediate node performs a data reception to consume 356 watts of energy and the data transfer consumes about 454 microwatts of energy.

The comparisons of the network lifetime for GPSR method and present invention ES for the different network sizes is indicated in Table 1 where the network scale represents the number of nodes in the WSN. The results show, network lifetime of the method of the invention is longer than that of the GPSR method under the two network sizes.

Table 1. Network lifetime at different network sizes (seconds)

Network size	300	400	100%
GPSR	29.04	29.04	16.4925
ES	147.04	147.04	83.5075

4.3. Data Transmission within the Wireless Sensor Network

The specific process of carrying out the security for present invention is that, firstly, at a current network scale, a certain proportion of the intermediate node is randomly set as the attack node; Then, the source node generating a packet and selecting the next hop node with the routing algorithm. When the attack node selected as the next hop node, it will tamper with the packet and forward it; finally, the destination node, received packet and tested to determine whether packet tampered during the network transmission.

The present invention has a packet loss rate as a basis for testing the performance of the patent reliability based on check code (CHEC) method and the method of the present invention ES, the packet loss rate [33] evaluated as shown on Eq. (4).

$$\mathrm{PLR} = \frac{\mathrm{EP}}{\mathrm{RP}} \quad (4)$$

Where, RP is the destination node as $Sink\ node$ for the number received packets, EP is the number of packets that have tampered. In the case of fixed network size, PLR smaller, indicates the destination node.If the number of packets that correctly received is less, the worse the security of the network.

In the experiment, the initial security degree of the intermediate node is 10, the network scale is400, and Table 2 indicates the packet loss rate under different attack nodes respectively. The experimental results indicates that the packet loss rate of the method of the present invention ES is less than that of the CHEC method at different attack node ratios.

The watermark embedding into the data packet transmitted, then, based on the distance, the security and the residual energy, the node quality evaluation introduced to optimize the next hope node. Thus, by judging whether the data packet tampered during transmission to receive data packets in the watermark detection, and adaptive adjustment of the node degree of safety, ultimately achieve safe and effective data transmission in WSNs.

Table 2. Packet loss rates at different attack nodes

(attack node ratio)	4%	5%	6%	7%
CHEC	0.5549	0.6515	0.6768	0.7447
ES	0.2878	0.4747	0.5535	0.7174

5. Results and Evaluation

The results shown that GPSR use $29.04seconds$ for network size of $300\ and\ 400$ which is about 16.4925% less while the present invention method ES use the same network with $147.04second$ which is about 83.5075% processing time as shown table 1. The packet loss rate indicates that $CHEC < ES$ that means CHEC has an improvement for as 4% is

0.5549 to 0.7447 for 7% compared to present invention ES which shown packet received is less as for 4% is 0.2878 and for 7% is 0.7174 that means the worse security of the network as presented table 2.

The simulation results show that the rate of nodes against the network lifetime for the GPSR and S remain $63seconds$ for percentages from 4% to 7%. The E reach about 40second and the SE is less than 40second throughout percentages from 4% to 7% as shown Fig.6.

When applying an attack for simulation, the GPSR remain constant unchanged based on the packets received while the S, E and SE increasing more comparatively with the security as shown Fig.7,

The GPSR consume only $25seconds$ and remain unchanged for the whole network packet processing which consist 1000 $nodes$. The S, E and SE keep on increasing as network increasing to 1000 numbers on network size as shown in Fig.8

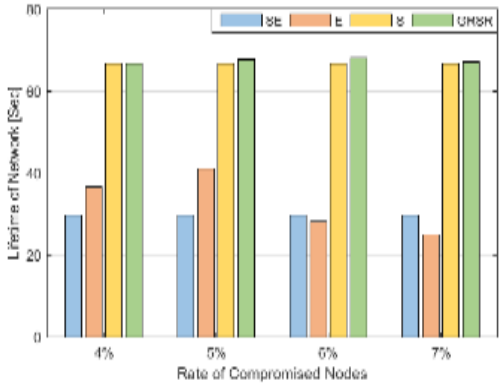

Fig.6: output results show number of nodes against energy lifetime

6. Energy Lifetime Evaluation

The average for nodes residua energy shows that the GPSR is above0.185, S is above 0.18 but less than 0.185 and the energy is constant for E at least 0.16 while the security 0.16 . That mean longer the network life, the more energy used as shown in Fig. 9.

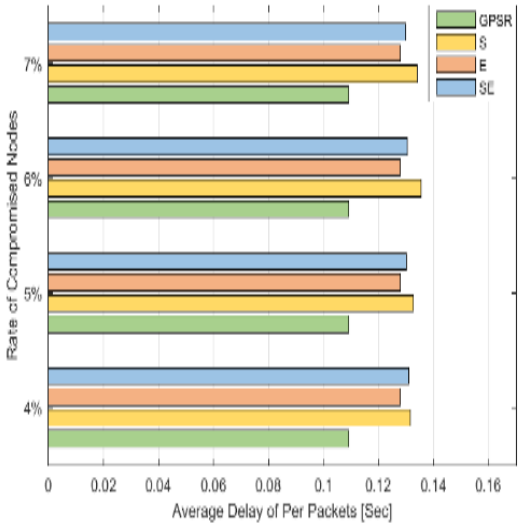

Fig. 7: output results with an attacker against energy and security

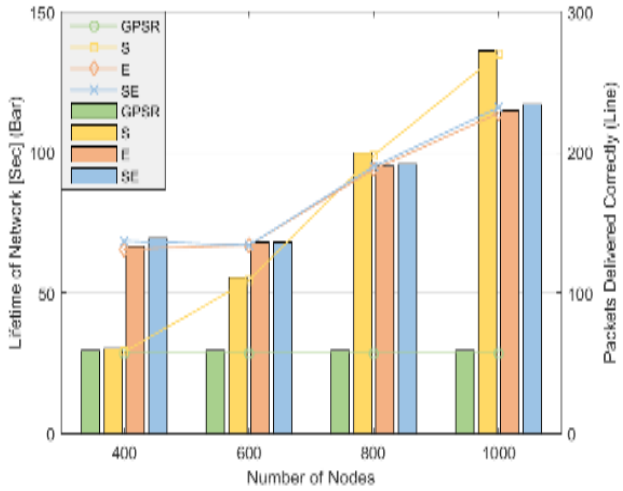

Fig.8: output results without an attack with node against Network lifetime

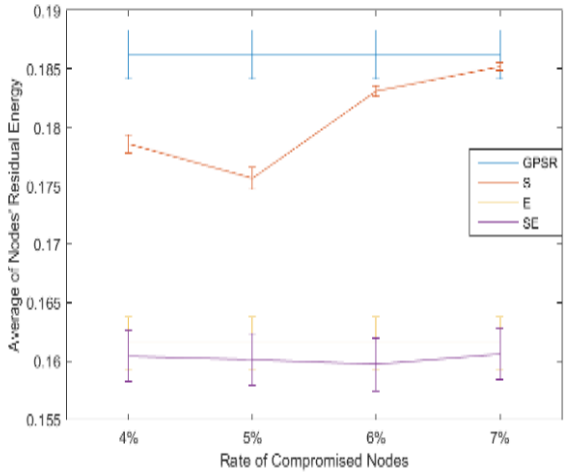

Fig.9: Output results shown the Node against the energy lifetime

7. Conclusion

This article proposes energy conservation lifetime using the GPSR and data security through transmission medium using the watermark technology in WSNs.

The GPSR shows that for a network size of 300 and 400 process the packets with only 16.4925% while the ES with the same network process with 83.5075%. That indicates ES consume more time processing the same data that will consume more power for processing.

The packet loss rate indicates improvement for CHEC as for 4% is 0.5549 to 0.7447 for 7% compared to present `invention ES` which shown packet received is less as for 4% is 0.2878 to 0.7174 for 7%. The experimental results indicate that the packet loss rate of the method of the present invention ES is less than that of the CHEC method at different attack node ratios.

The simulation results indicate that the GPSR is more accurate for routing because it processes data packet in less time for different simulation and when tested without an attacker the GPSR remain lower constant while the secure indicates highest level of data packet transmission for lifetime packets without an attack. Thus, the invention methods based on the digital watermark techniques ensure the ultimately achieve safe, secure and effective data transmission and GPRS maintain the energy lifetime within the WSNs

Author also present some review article about techniques methods, which used to reduce energy consumption and energy harvesting within WSNs

Acknowledgments

The author acknowledge the financial support received from China Scholarship Council (CSC) and Xidian University for their support and encouragement in carrying out this research work under supervision of Associate Prof. Lingling An from School of Computer Science and Technology, Xidian University.

References

[1] L. Wang and M. Huang, “Security and privacy in internet of things with crowd-sensing,” Journal of Electrical and Computer Engineering, 2017.

[2] A. Ali, Y. Ming, T. Si, S. Iram, and S. Chakraborty, “Enhancement of rwsn lifetime via firework clustering algorithm validated by Ann,” Information, vol. 9, no. 3, p. 60, 2018.

[3] M. Kocakulak and I. Butun, “An overview of wireless sensor networks towards internet of things,” in Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual. IEEE, 2017, pp. 1–6.

[4] M. Faheem and V. C. Gungor, “Energy efficient and qosaware routing protocol for wireless sensor network-based smart grid applications in the context of industry 4.0,” Applied Soft Computing, vol. 68, pp. 910–922, 2018.

[5] D. Block and U. Meier, “Discrete-event simulation of wireless coexistence for industrial applications: Requirements and solutions,” in Kommunikation und Bildverarbeitung in der Automation.Springer, 2018, pp. 163–176.

[6] S. Ehsan, K. Bradford, M. Brugger, B. Hamdaoui, Y. Kovchegov, Johnson, and M. Louhaichi, ``Design and analysis of delay-tolerant sensor networks for monitoring and tracking free-roaming animals," \emph {IEEE Transactions on Wireless Communications}, vol. ~11, no. ~3, pp. 1220--1227, 2012.

[7] [A. Singh and K. Gupta, “Preventing node replication attack in mobile wireless sensor networks,” in Information and Communication Technology for Sustainable Development. Springer, 2018, pp. 311–317.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (IoT): A vision, architectural elements, and future directions,” Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[9] P. G. V. Naranjo, Z. Pooranian, M. Shojafar, M. Conti, and R. Buyya, “Focan: A fog-supported smart city network architecture for management of applications in the internet of everything environments,” Journal of Parallel and Distributed Computing, 2018.

[10] E. S. Oliveira, J. P. J. Peixoto, D. G. Costa, and P. Portugal, “Multiple mobile sinks in event-based wireless sensor networks exploiting traffic conditions in smart city applications,” in 2018 IEEE 16th International Conference on Industrial Informatics (INDIN). IEEE, 2018, pp. 502–507.

[11] H. S. Fimbombaya, N. H. Mvungi, N. Y. Hamisi, and H. U. Iddi, "Performance evaluation of magnetic wireless sensor networks algorithm for traffic flow monitoring in chaotic cities," Modelling and Simulation in Engineering, vol. 2018, 2018.

[12] A. Mile, G. Okeyo, and A. Kibe, "Hybrid IEEE 802.15. 6 wireless body area networks interference mitigation model for high mobility interference scenarios," Wireless Engineering and Technology, vol. 9, no. 02, p. 34, 2018.

[13] H. Yan, H. Huo, Y. Xu, and M. Gidlund, "Wireless sensor network based e-health system-implementation and experimental results," IEEE Transactions on Consumer Electronics, vol. 56, no. 4, pp. 2288–2295, 2010.

[14] G. Fortino, H. Ghasemzadeh, R. Gravina, P. X. Liu, C. C. Poon, and Z. Wang, "Advances in multi-sensor fusion for body sensor networks: Algorithms, architectures, and applications: Guest editorial," 2018.

[15] S. Waharte and N. Trigoni, "Supporting search and rescue operations with uavs," in Emerging Security Technologies (EST), 2010 International Conference on. IEEE, 2010, pp. 142–147.

[16] G. Hoareau, J. J. Liebenberg, J. G. Musial, and T. R. Whitman, "Dynamically establishing a temporary safe route via a network of unmanned aerial vehicles," Feb. 20 2018, uS Patent9, 897,456.

[17] A. Sabata, K. Baumgartner, T. Jayet, J. Lawlor, and O. Cheiaru, "Cyber security: A system to monitor home wi-fi networks, "May 17 2018, uS Patent App.14/964,650.

[18] K. Ravinder and G. Rajender, "Recognition of authorized peoples in collage by using RFID technology with iot platform," IJITR, vol. 6, no. 4, pp. 8498–8500, 2018.

[19] P. R. Vamsi and K. Kant, "An improved trusted greedy perimeter stateless routing for wireless sensor networks," International Journal of Computer Network and Information Security, vol. 6, no. 11, p. 13, 2014.

[20] J. M. K. Attoungble and K. Okada, "A novel energy efficient routing protocol for wireless sensor networks: Greedy routing for maximum lifetime," IEICE transactions on communications, vol. 95, no. 12, pp. 3802–3810, 2012.

[21] L. Kong, J.-S. Pan, V. Snášel, P.-W. Tsai and T.-W. Sung, "An energy-aware routing protocol for wireless sensor network based on genetic algorithm," Telecommunication Systems, vol. 67, no. 3, pp. 451–463, 2018.

[22] M. Panda, "Security in wireless sensor networks using cryptographic techniques," American Journal of Engineering Research (AJER), vol. 3, no. 01, pp. 50–56, 2014.

[23] B. Harjito, V. Potdar, and J. Singh, "Watermarking technique for copyright protection of wireless sensor network data using lfsr and kolmogorov complexity," in Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia. ACM, 2012, pp. 208–217.

[24] V. Holub and T. Filler, "Methods for estimating watermark signal strength, an embedding process using the same, and related arrangements," May 10 2018, uS Patent App. 15/655,376.

[25] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on dwt, dct and svd for application in medicine," Multimedia Tools and Applications,vol. 77, no. 4, pp. 4863–4882, 2018.

[26] R. Soua and P. Minet, "A survey on energy efficient techniques in wireless sensor networks," in Wireless and Mobile Networking Conference (WMNC), 2011 fourth Joint IFIP.IEEE, 2011, pp. 1–9.

[27] M. Byamukama, J. N. Nannono, K. Ruhinda, B. Pehrson, M. Nsabagwa, R. Akol, R. Olsson, G. Bakkabulindi, and E. Kondela, "Design guidelines for ultra-low power gateways in environment monitoring wireless sensor networks," in AFRICON, 2017 IEEE.IEEE, 2017, pp. 1472–1478.

[28] A. Nungu, R. Olsson, and B. Pehrson, "On powering communication networks in developing regions," in Computers and Communications (ISCC), 2011 IEEE Symposium on. IEEE, 2011, pp. 383–390.

[29] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey, "Ad hoc networks, vol. 7, no. 3, pp. 537–568, 2009.

[30] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks, "in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 3. IEEE, 2003, pp. 1713–1723.

[31] D. Drusvyatskiy, H.-L. Lee, G. Ottaviani, and R. R. Thomas, "The Euclidean distance degree of orthogonally invariant matrix varieties," Israel Journal of Mathematics, vol. 221, no. 1, pp.291–316, 2017.

[32] D. Goldsby, "Area of a circle," in Pedagogy and Content in Middle and High School Mathematics. Springer, 2017, pp.99–100.

[33] J. Wang and Y. bin Hou, "Packet loss rate mapped to the quality of experience," Multimedia Tools and Applications, vol. 77, no. 1, pp. 387–422, 2018.

Gaudence Stanslaus. He received proficiency in certificate level in Multimedia for Music Production from SAE College Bangkok, Thailand in 2013 and Diploma in Full Computer Engineering (FTC) from Dar Es Salaam Institute of Technology, Dar Es Salaam, Tanzania East Africa in 2003 and then Bachelor of Engineering (BEng) in Electronics and telecommunication from Dar Es Salaam Institute of Technology, Dar Es Salaam, Tanzania East Africa in 2007. Master in Engineering (MEng), Information

and Communication from Chongqing University, Chongqing, China in 2011. He is currently pursuing PhD with School of Telecommunications Engineering, Xidian University, Xi'an, China. His research interests include communication networks, Multimedia Security, Information security and wireless sensor Network.