SECURED TRANSMISSION IN DOUBLE CLUSTERED HETEROGENEOUS MOBILE WIRELESS SENSOR NETWORK

T. Preethiya
Research Scholar. Department of ECE.
Kalasalingam Academy of Research and Education,
Srivilliputtur, (India).
E-mail: preethiya.t@gmail.com ORCID: https://orcid.org/0000-0003-3504-1884

A. Muthukumar
Associate Professor. Department of ECE.
Kalasalingam Academy of Research and Education,
Srivilliputtur, (India).
E-mail: muthuece.eng@gmail.com ORCID: https://orcid.org/0000-0001-8070-3475

S. Durairaj
Principal. Dhanalakshmi Srinivasan Engineering College.
Perambalur, (India).
E-mail: rajsdr@rediffmail.com ORCID: https://orcid.org/0000-0002-7104-687X

Recepción: 05/12/2019 **Aceptación:** 13/01/2020 **Publicación:** 23/03/2020

Citación sugerida:
Preethiya, T., Muthukumar, A., y Durairaj, S. (2020). Secured Transmission in Double Clustered Heterogeneous Mobile Wireless Sensor Network. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Edición Especial, Marzo 2020*, 51-67. http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

Suggested citation:
Preethiya, T., Muthukumar, A., & Durairaj, S. (2020). Secured Transmission in Double Clustered Heterogeneous Mobile Wireless Sensor Network. *3C Tecnología. Glosas de innovación aplicadas a la pyme. Edición Especial, Marzo 2020*, 51-67. http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

ABSTRACT

In recent years, Mobile Wireless Sensor Network (MWSN) has derived the attention of vendors and researchers as it being the state-of-art technology in the areas of battle field surveillance, medical and military application etc. The Mobile Double Cluster Head-Particle Swarm Optimization (MDCH-PSO) algorithm is proposed for optimization in hybrid mobile network with a heterogeneity. This paper proposes an algorithm Secure-MDCH (S-MDCH) to improve the security aspects of MDCH-PSO algorithm. In S-MDCH, inter-cluster and intra-cluster key generation algorithms are explained to prevent the network from malicious node attack and CH compromising. This ensures secure communication in the network. A unique mobile key '' is used by all nodes to avoid malicious node from entering the cluster through handoff and to prevent 'information learning'. Simulation results shows that packet delivery ratio of the proposed algorithm is 8.25% higher than LEACH-M and average residual energy is improved by 2.802%.

KEYWORDS

MWSN, Mobility, Heterogeneous, Security, Inter-cluster, Intra-cluster keys.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

1. INTRODUCTION

MWSN is a collection of an infrastructure less, self-organizing nodes with sensors to detect event occurrence that are connected wirelessly to form an arbitrary topology. The basic need of a network is to ensure a reliable data transmission, higher connectivity, lower energy consumption and increased life time. Many existing WSN application such as habitat monitoring, surveillance and medical application adopts mobility in its execution. Though, mobility makes the network complex its need make it as an advantage. Many research has revealed that mobility characteristics improves the overall network and QoS performance of the network.

1.1. MWSN ARCHITECTURE

As shown in Figure 1, in every sensor node a sensing unit, processing unit, transmission unit and a power unit are mandatory for its operation. The blocks mobilizer and position finding system are optional which can be activated based on the application. Enabling these optional blocks has provided a new paradigm to the sensor network 'Mobile Wireless Sensor Network' that can be used in many application creating a base for IoT and pervasive computing. The sensing unit comprises of sensor and analog-digital conversion circuit. The sensor can be selected from the wide range based on the application. The processing unit process the incoming data and stores it in a register. The transmitter is a communication model which provides radio transmission in the ground surface. The two components motor and chassis of mobilizer enables the node movement. These components are selected depending on the application.

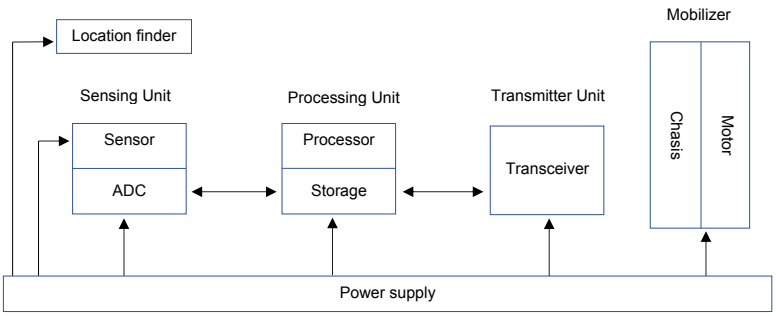

Figure 1. Architecture of MWSN.

http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

The MWSN node move over air, water or ground as application demands. Similarly, the chassis used also differs. The wheels, the caterpillars and the walking legs are the major options for movement of nodes in ground. To transform the electrical energy into the mechanical energy required for wheel or caterpillar rotation or leg movement, the mobile node use the motors. Each node uses two motors for its direction change. According to Gungor and Hancke (2009), Srivastava (2010) and Rathee, Singh and Nandini (2016), the challenges of MWSNs are identified as processing speed, network heterogeneity, scalability, hardware cost, deployment, Size of memory and battery, balanced traffic, dynamic topology, mobility, coverage, energy consumption, localization, node failure, QoS, fault tolerance, wireless connectivity, and security. The addition of security features to the MWSN's make it more compatible.

Messai (2014) and Singh, Singh and Singh (2016) has identified the possible security threats in mobile networks as:

Malicious node attack- An intruder can act as a handoff node and falsify the local data

Being a mobile network there will be a frequent topology change and it is handled by handoff. In this case both hard and soft handoff takes place. In such case, a malicious node can act as a handoff node from adjacent cluster and transmit false event data to the female node thereby wasting the resources.

Learning information table

A malicious node can learn entire cluster details through female node communication that may violate message confidentiality and authentication.

Compromised CH attacks

The CH node is compromised by the attacker which creates black hole attack, selective forwarding attacks in the network.

This paper proposes an intra-cluster and inter-cluster key generation algorithm for double cluster head heterogeneous mobile hybrid network. In general, mobility is the movement of node from one place to the other. Security is an important aspect in any mobile network

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

as it changes its topology dynamically. This allows the intruders to spoof the transmitted information and create other attacks in the network. For a DCH network, a malicious node can easily enter and modify the information table. This is avoided by a unique mobile key by the mobile node.

2. LITERATURE SURVEY

Xuegong and Chen (2010) have introduced a 'Double Cluster-Head topology Control Algorithm' (DCCCA) for a heterogeneous network. MCH is selected based on weight. Here, Main CH (MCH) collects the data and transmitted by an Assistant CH (ACH) to the next CH. A chain based algorithm 'Power-Efficient Gathering in Sensor Information Systems with Double Cluster Head (PDCH)" is proposed by Linping, Wu, Zhen and Zufeng (2010), where the cluster heads are classified as MCH and secondary CH. The parameters such as energy and distance to CH were used for CH selection. A node with higher tag value and with more than two neighbors is elected as MCH and any one of its neighbors in the next level is elected as secondary CH. Because of this, node that is far away from CH node takes too much energy to send its own data to cluster head from network.

Xiao and Deng (2010) recommended a 'Double Head Static Cluster' (DHSC) algorithm where the problems related to uneven distribution of nodes are addressed. The MCH is selected in thick and ACH in thin area and they are used to reduce single cluster head's energy consumption. An algorithm called 'Multiple Cluster-heads Routing Protocol' (MCHRP) is proposed by Da, Liu, Jiao and Yue (2011). This MCHRP algorithm uses max-min approach for the election of CH. The MCH selection is based on residual energy and frequency of being CH and Vice CH (VCH) election is based on residual energy, distance between node to CH, distance between node to base station and frequency of being CH.

Suresh and Selvakumar (2014) have proposed the SKADC algorithm uses an inter-cluster and intra-cluster keys to provide security for static WSN. It uses SHA-1 MAC for node authorization. The digest size of SHA-1 MAC is 20 bytes and 80 steps to create a digest size. In real time, TinySec frame work will have 29 bytes of information to transmit the message. With SHA-1 MAC, the remaining 9 bytes are left blank which results in waste of resources. This algorithm is proposed for double cluster architecture. Four different keys

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

are generated in intra-cluster key generation. A multiplicative element is obtained to avoid compromising of node.

In literature, numerous algorithms are proposed for double CH selection and energy efficiency. The above study explains double cluster head mechanism for wireless sensor network. The existing algorithms do not focus the security aspect of the network. A mobile network with double cluster head has to face the more security issues than the single clustered architecture. This paper explains about the security aware energy efficient double cluster head algorithm for a mobile network.

The contribution of this paper given below.

1. It is proposed for double clustered heterogeneous hybrid mobile network.
2. It uses SHA-224 algorithm for MAC generation. The number of keys generated in intra cluster communication is reduced.
3. A unique individual key is given to all node by F nodes for transmitting.
4. A mobility key is also generated to learn mobility in the network.
5. A unique multiplicative element is obtained periodically to prevent attacker from knowing keys.

3. PROPOSED WORK

3.1. S-MDCH

There are four phases in the Secure-MDCH (S-MDCH) algorithm as shown in Figure 2. In this algorithm, there are two CH namely male CH (Temporary CH) that is elected among the member node and female node is heterogeneous immobile node that acts as the backbone of the network.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

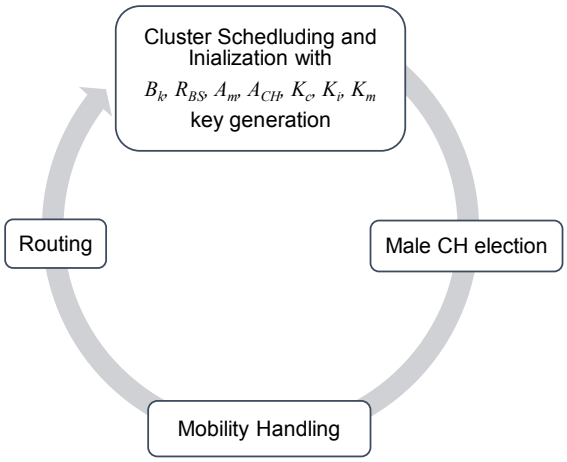

Figure 2. Phases of S-MDCH algorithm.

a) *Cluster scheduling algorithm and initialization phase*

In this phase, initial clustering is done (i.e.) member nodes are registered or scheduled with the female node using the received signal strength of every node to get connected with female node. The HELLO_PKTS are generated and flooded by the female sensor node. It consists of the source address of the female sensor node and information fields. Similarly, the REPLY_PKTS from each node contains source and destination address field, information field. Each node sends its node id, residual energy, one hop neighbors, and distance to female node in its information field and time stamp in its REPLY_PKTS. The possible security issue in this phase is 'learning information table'. A malicious node that acts as member node may register with female node and acquire its cluster details.

The female node floods a HELLO_PKT to its member node which in turn sends a REPLY_PKT which has its digital signature in addition to the data. The female node uses a verifying algorithm to the data received and if the result is true, data from that member node is accepted and store in its table.

b) *PSO based male CH Selection phase*

The temporary male selection is done using Particle Swarm Optimization. The fitness value is calculated as follows:

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

$$fitness\ (i) = w_1 E_{residual}(i) + w_2 Distance_{\ to\ female} + w_3 Node\ density(i) \quad (1)$$

$$E_{residual} = E_{initial} - (E_{Tx} + E_{Rx} + E_{mobile}) \quad (2)$$

$$Distance_{\ to\ female} = Tx_{range} \times M_s \quad (3)$$

$$Node\ density = \frac{Node_{degree}}{\pi \times \varphi} \quad (4)$$

where w_1, w_2 and w_3 are constants between 0 and 1.

c) *Mobility handling Phase:*

The female node updates its "information table" after every transmission by HELLO-REPLY packets. In short, if a node does not reply, the female node consider it as an 'away node' and remove its data from the table after waiting till its next HELLO-REPLY packets. Meanwhile, if a new node enters the cluster, female node obtain it's K_m and decrypts that to authenticate that node. Finally, female node consider it as the 'recent node' and update its information in the table through the subsequent HELLO-REPLY message.

d) *Routing Phase:*

The female node directly gathers the information from its member node that are registered in the table. The routing phase involves the intra and inter-cluster key generations for secure transmission of data. The female node gathers the event occurrence from all the nodes and aggregate it D_{agg}. This is forwarded to male CH to reach the base station with public and private keys. The algorithm is described in next sub section.

e) *SHA-224 algorithm:*

The data field is 29 bytes for a TinySec authentication frame work. So, a message digest used for authentication should be 29 bytes. The digest sizes of SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 are 20, 28, 32, 48, 64 bytes respectively. The SHA-256, SHA-384 and SHA-512 are excluded since their digest size exceeds the limit. So, SHA-1 and SHA-224 are the choices. In an event sensing mobile environment the computation time should be less. Nunoo-Mensah, Boateng and Gadze (2015; 2017) has clearly proved that SHA-224 has less execution time when compared with SHA-1. So, we have adopted SHA-224 algorithm in S-MDCH for MAC generation.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

3.2. INTER CLUSTER KEY GENERATION

1. Base station broadcasts initial B_k to Female *'F'*

$$B_k:\{IM_i||SN_i||L_P\}$$

$$if\ H(SN_i)= SN_{i-1}$$

then

$$B_k\ is\ autorized$$

$$else$$

$$F_i\ drops\ B_k$$

$$endif$$

2. Update L_P to reach base station

3. After recievig B_k, F_i sends reply R_{BS} to base station

$$R_{BS}=\{E(ID(F_i), K_r, K_{pri}(F_i)||E(MAC(R_e||ID(F_i), K_r, K_{pri}(F_i))))\} \quad (4)$$

4. BS after recieving R_{BS} from CH validates the message and generates an authorization message (A_m) to every CHs.

5. BS after K_r from R_{BS} and adds it to A_m and univasts to Female nodes.

$$A_m=\{ID(F_i), K_r, K_{pri}(F_i)||E(MAC(R_e||ID(F_i), K_r, K_{pri}(F_i)))\} \quad (5)$$

6. CH upon recieving the A_m verifies and decrypts it and generates level key (KLi) for its child cluster heads. Then if forwards the cluster head authorization message A_{CH} to child cluster heads.

$$A_{CH}=\{ID(F_i)||E(KLi, K_r)\} \quad (6)$$

http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

3.3. INTRA-CLUSTER KEY GENERATION

7. 'F' broad casts routing message R_{req} to its m_i.

8. Each mi broadcasts the R_{req} message to its neighbors and obtains the hop distance to reach 'F'.

9. Nodes with less number of hops to reach F will act as Male node 'M' and if twho nodes have same hop count a node with less mobile speed is eleccted as 'M'.

10. m_i broadcasts R_{req} message in the reverse path trasversed by request message.

11. The following kets are generated for secure communication within the cluster.

    a. Cluster key K_c - to be shared with entire cluster.

    b. Individual key K_i - to be shared with F.

    c. Mobility key K_m - generated when a new node joins the cluster due to mobility.

12. To prevent attacker from confronting the keys, it is generated by a source multiplicative element 'z' with a random key values.

    a. Note: These keys changes with when 'z' changes.

13. F can request BS for new 'z' periodically which avoids node compromising.

4. RESULTS AND DISCUSSION

Simulation area is assumed to be 600 m×600 m with 50 nodes distributed randomly. Sink node is placed at (300,300) to gather the occurrence of events from various locations. The mobility model used is Random Way Point model. This is chosen because it is a model that can use pause time between changes and speed. The simulation results are recorded at mobility speed 20m/sec to study the performance of network. The pause time is set to 50 sec. The initial energy of member node is set to 2 Joules and a female node is 10 Joules. Table 1 shows the simulation parameters considered for the energy model of the network and simulated using network simulator 2.35.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

Table 1. Simulation parameters.

Parameter	Value
Deployment	Random
Energy Consumption per bit	50 nJ/bit
εfs	10 pJ/bit/m2
εmp	0.0013 pJ/bit/m4
Data packet size	512 bytes
C1 and C2	2
W	0.9

A malicious node has been introduced to study the performance of the network. Figure 3 shows the packet delivery ratio against the offered load. The delivery ratio gets dropped as the offered load increases in the network in both algorithms. The delivery ratio is 8.25 % higher than the LEACH-M algorithm. The obtained PDR is consistent during less offered load because of the high pause time which avoids topology change for 50 sec. This will prevent any malicious node from entering the cluster due to handoff. Also, the entire transmission takes place in a stable energy efficient secured path. The data transmission takes place using a unique private key and hash value for each transmission. Further increase in load, will create congestion in the network thus PDR decreased. This can be improved by varying the mobile speed of each node.

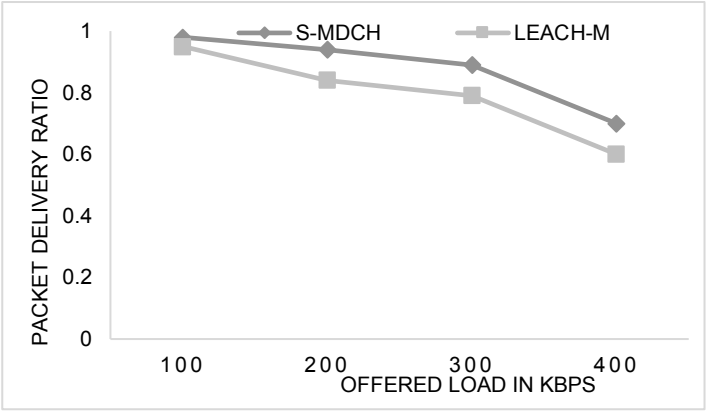

Figure 3. PDR versus Offered load.

Generally in mobile network, mobility is a major reason that contributes to packet drop. If the route to destination is not available then the packets drop at the source node and if the next hop is not available then packet loss occurs at intermediate nodes. Also, malicious

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

node may cause more packet dropping which forwards only the selective packets to the destination and drops the other. This affects the message integrity at the base station. In the proposed algorithm, the malicious is node is identified in the registration phase. Even if malicious node receives the packet it is not able to modify the data packet. From the Figure 4, it seen that packet loss is 8% higher in LEACH-M when compared to the S-MDCH. This is because LEACH-M has not been designed to provide security rather it simply carry forward the packet. As the offered load increases, the packet loss increase in both algorithms, because higher load with more mobile nodes causes congestion and frequent change in path to the destination. However, this is reduced by the pause time of the nodes and some nodes still may cause it to happen. (i.e.) a node in the path has completed its 50 sec pause time during transmission. The other way of improving packet loss is by adhering varying mobile speed for each node.

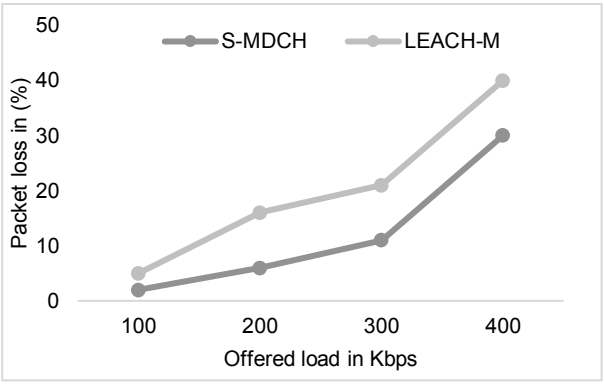

Figure 4. Packets dropped versus Offered load.

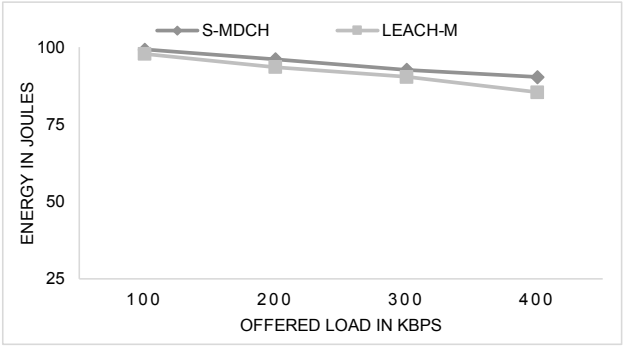

Figure 5. Average residual energy versus Offered load.

http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

When compared to static node, mobile node spends one part of its energy in mobility of node. This is may vary due to additional components attached to mobilizer unit. Figure 5 represents the average residual energy of member nodes (initial energy is 2J) in the network. The total number of nodes is 50*2J=100J. As shown in Figure 5, the average residual energy of the network in S-MDCH is 2.802% higher than the LEACH-M algorithm. In S-MDCH algorithm, a time-stamping based handoff mechanism is used whereas in LEACH-M, a simple handoff mechanism is used. The reduced number of key generation reduces the overhead transmission which results in effective energy minimization.

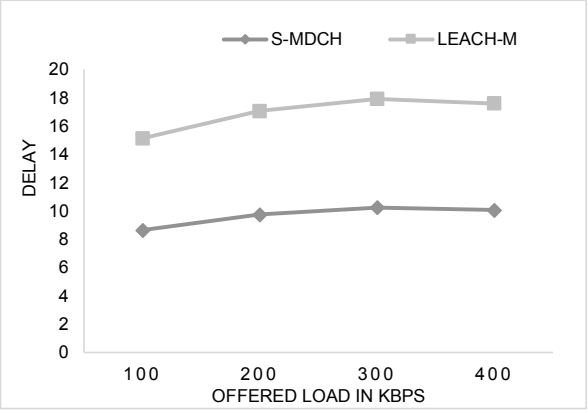

Figure 6. Delay versus Offered load.

Figure 6 shows the Offered load Vs delay. From the Figure 6, it is analyzed that average delay of S-MDCH is 7.25 times less than LEACH-M algorithm. The reason behind this is, in LEACH-M algorithm the CH monitors the member nodes and generates all inter-cluster and intra-cluster keys for secured communication. In the proposed S-MDCH algorithm inter-cluster keys are generated by the female node and intra-cluster keys by the member nodes and female. The female node generates the cluster key and unicasts it to all member nodes. Similarly, if a node wants to transmit it uses its individual key rather than using neighbor keys. Therefore all nodes concentrate on communication rather monitoring.

5. CONCLUSION

This proposed S-MDCH algorithm improves the security aspects of MDCH-PSO algorithm. The proposed algorithm uses SHA-224 algorithm which reduces the execution

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

time in a TinySec framework. The number of keys used in intra-cluster communication is reduced and a mobility key is introduced to authenticate the mobile node during handoff. Simulation results shows that packet delivery ratio of the proposed algorithm is 8.25% higher than LEACH-M, average residual energy is improved 2.802 % and delay by 7.25 times less than LEACH-M algorithm. In future, algorithm can be adopted to the network with varying mobility speeds.

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

REFERENCES

Da, T., Liu, X., Jiao, Y., & Yue, Q. (2011). A load balanced multiple Cluster-heads routing protocol for wireless sensor networks. *IEEE 13th International Conference on Communication Technology, Jinan, 656-660.*

Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics, 56*(10), 4258- 4265. https://doi.org/10.1109/TIE.2009.2015754

Linping, W., Wu, B., Zhen, C., & Zufeng, W. (2010). Improved algorithm of PEGASIS protocol introducing double cluster heads in wireless sensor network. In *International Conference on Computer, Mechatronics, Control and Electronic Engineering, Changchun, pp. 148-151*. https://doi.org/10.1109/CMCE.2010.5609618

Messai, M. L. (2014). Classification of Attacks in Wireless Sensor Networks. *International Congress on Telecommunication and Application' 14 University of A. MIRA, Bejaia, Algeria, pp. 23-24.*

Nunoo-Mensah, H., Boateng, K. O., & Gadze, J. D. (2015). Comparative analysis of energy usage of hash functions in secured wireless sensor networks, *International Journal of Computer Applications, 109*(11), 20–23. https://doi.org/10.5120/19233-0968

Nunoo-Mensah, H., Boateng, K. O., & Gadze, J. D. (2017). Tamper-aware authentication framework for wireless sensor networks. *IET Wireless Sensor Systems, 7*(3), 73-81.

Ramasamy, V. (2017). *Mobile Wireless Sensor Networks: An Overview. Wireless Sensor Networks - Insights and Innovations,* Chapter 1. https://doi.org/10.5772/intechopen.70592

Rathee, A., Singh, R., & Nandini, A. (2016). Wireless sensor network—challenges and possibilities. *International Journal of Computer Applications, 140*(2). https://www.ijcaonline.org/archives/volume140/number2/24563-2016909221

Singh, R., Singh, J., & Singh, R. (2016). Attacks in wireless sensor networks: a survey. *International Journal of Computer Science and Mobile Computing, 5*(5), 10-16.

Srivastava, N. (2010). Challenges of next-generation wireless sensor networks and its impact on society. *Journal of Telecommunications, 1*(1), 128-133.

Suresh, D., & Selvakumar, K. (2014). Secure Key-Tree Architecture for Double Cluster Based Routing in Wireless Sensor Network. *International Journal of Applied Engineering Research, 9*(22), 16143-16157.

Xiao, Y., & Deng, L. (2010). A double heads static cluster algorithm for wireless sensor networks. *2nd Conference on Environmental Science and Information Application Technology, Wuhan, pp. 635-638*. https://doi.org/10.1109/ESIAT.2010.5568343

Xuegong, Q., & Chen, Y. (2010). A control algorithm based on double cluster-head for heterogeneous wireless sensor network. *2nd International Conference on Industrial and Information Systems, Dalian, pp. 541-544*. https://doi.org/10.1109/INDUSIS.2010.5565790

 http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67

http://doi.org/10.17993/3ctecno.2020.specialissue4.51-67