Circuits and Systems, 2016, 7, 1845-1855
Published Online June 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.78159

GSTP: Geographic Secured Two Phase Routing Using MD5 Algorithm

B. Prathusha Laxmi*, A. Chilambuchelvan

R.M.K. Engineering College, Anna University, Chennai, India
Email: *prathushakrishnaa@yahoo.com, chill97@gmail.com

Received 16 April 2016; accepted 10 May 2016; published 22 June 2016

Abstract

Secured Two Phase Geographic Greedy Forwarding (SecuTPGF) is a geographic greedy forwarding protocol for transmitting multimedia data stream in Wireless Multimedia Sensor Networks (WMSN) in a secure and reliable manner. Cryptographic and MAC authentication mechanisms are used to implement security for both node and message authentication. In this paper, a modified version of SecuTPGF, the GSTP routing provides security for both node and message authentication by using MD5 algorithm with a reduced computation power. In SecuTPGF, two different algorithms are used for node and message authentication, and GSTP routing uses "MD5Algorithm" for both node and message authentication. Using MD5 algorithm for node and message authentication, the average number of transmission paths increased and average number of hops used for transmission decreased when compared to the SecuTPGF. By conducting security analysis & evaluation experiments, the effectiveness of GSTP routing algorithm is proved.

Keywords

GSTP, MD5, MAC, Security, Routing, WMSN

1. Introduction

Traditional wireless sensor networks provide information for events such as temperature, sound, pressure, etc. Multimedia sensor networks provide enhanced information for events such as video & audio streams. Transmitting multimedia information through the wireless network is a challenging task due to its limited power resource. Some of the wireless multimedia sensor network applications are health care, industrial process control, and traffic congestion avoidance system.

Geographic routing is a routing principle that uses geographic position information instead of the network ad-

*Corresponding author.

How to cite this paper: Laxmi, B.P. and Chilambuchelvan, A. (2016) GSTP: Geographic Secured Two Phase Routing Using MD5 Algorithm. *Circuits and Systems*, **7**, 1845-1855. http://dx.doi.org/10.4236/cs.2016.78159

dress. In geographic routing, each node determines its own location and the source possess information about the location of the destination. Greedy forwarding technique forwards the multimedia message to the destination in each step using the local information available in the intermediate 1-hop neighbouring nodes. The selection of 1-hop neighbouring node for forwarding is the one having minimum distance to destination in each step.

Wireless sensor network can be represented as a graph G(V, E), where V represents a set of sensor nodes and E is a set of links. Two Phase Geographical greedy forwarding [1] is a routing protocol for wireless multimedia sensor networks where routing is performed in a two-phase. The first phase is the geographic forwarding which is responsible for finding the possible routing path. $P_{nth} = \{V_{Pn1}, \cdots, V_{Pnm}\}$ inside the graph $G_{available}(V_{available}, E_{available})$ from the source nodes to the base station. The second phase is the path optimization which is responsible for optimizing the identified routing path with least number of hops. P_{nth} optimized $= \{V_{0Pn1}, \cdots, V_{0Pnm}\}$ (P_{nth} optimized $\underline{C}P_{nth}$) to optimize the found routing path with less number of nodes.

SecuTPGF provides the security during the identification of 1-hop neighbours & route discovery. In paper [2], security is provided by authenticating node with symmetric key establishment. Key exchange is done by "Identify-Based Non Interactive Key Distribution scheme (ID-NIKDS)". Message is authenticated by MAC algorithm.

Various functional and non-functional requirements for simulating WSN have been reviewed to evaluate the performance of the routing protocol. In paper [3], Hardware resources such as CPU and memory usage are considered as one of the main parameters to select most suitable simulators for wireless sensor networks. Other parameters such as routing and energy are also considered. For real deployment, small scale test bed is sufficient to validate the test results. Efficiently transmitting streaming data deals with two basic problems: 1) collecting required data; 2) minimizing transmission delay within a short duration of expected network life time. In paper [4], two algorithms are used to solve those problems. Maximum Streaming Data Gathering and Minimum Transmission Delay algorithms should be executed during the initialization phase of every node to choose appropriate Transmission Radius. Once the transmission radius is selected appropriately, the above said basic problems can be avoided.

For designing and validating routing algorithms, NetTopo simulation tool is widely used for simulating real wireless communication environments in terms of accuracy and security. It is a platform independent Tool. Limitations such as large scale deployment and capable of replicating the same environment are challenging tasks in any simulator. This can be overcome by using NetTopo Simulator [5], both the limitations are considered and it is possible. Implementing new algorithms in NetTopo Simulator is a three-step process [6]: 1) rewriting new node java class; 2) rewriting a new topology java class and registering it with NetTopo; 3) implementing new algorithm by using the existing algorithm.

Various techniques and algorithms are used for the secured communication in sensor networks [7]. The strength of the algorithm depends upon the key management and the cryptography type.

In paper [8], various routing metrics in WSN are reviewed. As sensor nodes have limited power capability, routing power metrics plays a major role.

In paper [9], current status on the security aspects of Wireless Multimedia Sensor Networks are given. Denial of Service attacks is a challenging problem in WSN.

2. Problem Statement

In [1], the routing algorithm has no security mechanism, malicious nodes can perform any attacks such as insider and outsider adversary attacks. In [2], the routing algorithm prevents unauthorized node from joining the network by verifying the origin and integrity of the data. This can be done by using message authentication code (MAC). Ex: Hash-based Message Authentication Code (HMAC) and a key are shared between the two parties. In SecuTPGF routing algorithm both the node and message authentication is done by Cryptographic & MAC mechanism respectively, which requires more computation, thereby more energy consumption.

In GSTP routing algorithm, both the node and message authentication is done by MD5 algorithm, which requires less computation, thereby the energy and power conservation is less when compared to the SecuTPGF algorithm.

3. Hashing Algorithm—MD5

Hashing Algorithms are widely used to check the integrity of the transmitted message by the computation of

unique hash value for the message being transmitted. A Cryptographic hash function calculates a constant length hash value for a given variable length of message is one of the notable properties which make it suitable for the purpose of authentication. In general, the nodes having their unique ID and may generate surely distinct hash values that correspond to each of the node. The need to have a hashing algorithm to compute additional hash value may inquire additional computational power. Computational power increases the power consumption which is of major concern in multimedia sensor nodes which are deployed in locations where power supply is impossible.

Hashing algorithms are characterized by their consumption of energy, speed at which they calculate the hash values and their collision resistance capabilities. The First two issues is one of the major concerns in wireless sensor networks where the collision resistance is of least importance since it takes nearly large number of nodes to deploy to create a scenario for collision which is infeasible.

The data input (message of any length) is sent to MD5 algorithm to create 128-bit message digest for verifying data integrity. The message digest created, acts as a finger print for individual.

MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321.

Pseudo Code

Step 1 Padding: The original message length (in bits) is congruent to 448, modulo 512, when padding bits are appended. The padding rules are:

- The first bit to be padded with the original message should always be "1" bit.
- "0" to be padded for the remaining bits, until the length of message is 64 bit lesser than multiple of 512.

Step 2 Increasing the Length: The length of the original message should be in bytes; hence 64 bit are appended at the end of padded message.

1) 64 bit binary format is obtained by converting the original message in bytes. In case of exceeding the length, low-order 64 bits are only used.

2) 64 bit binary format length is divided into two words (32 bit each). Specify the low-order word first and then followed by the high-order word at the end.

Step 3 Initializing MD Buffer: MD5 algorithm needs a 128-bit buffer with initial value. Initializing buffer rules are:

- The buffer is divided into four words named as A B, C and D (32 bit each).
- 0x67452301 is initialized to Word A.
- 0xEFCDAB89 is initialized to Word B.
- 0x98BADCFE is initialized to Word C.
- 0x10325476 is initialized to Word D.

Step 4 Processing Message in 512-bit Blocks: This is the important step of MD 5 algorithm. In this step, it loops through padded and appended message in blocks (512 bit each). For each input block, four rounds of operations and for each round sixteen operations are performed.

Step 5 Output: Buffer words A, B, C and D's output are in sequence with low-order byte first.

In this paper, base station gets the ID of the each of the sensor node. Hash the ID and store it as an attribute in the sensor node. This Hash value is used for node and message authentication.

4. Geographic Secured Two Phase Routing Using MD5 Algorithm

GSTP routing algorithm consists of three phases 1) Initialization & setup 2) Identifying secured 1-hop nodes 3) Routing through secured 1-hop nodes.

4.1. Initialization & Setup

This stage is to be executed by the base station by an authenticated authority using its own facilities for processing in order to minimize the power consumption of the other nodes. After deploying the sensor network, base station gets the ID of each of the sensor node for processing. Initially, the ID of the sensor node is hashed by using MD5 algorithm and the computed hash value is stored as an attribute in the sensor node as shown in **Figure 1**.

Once, the initialization and setup phase is completed, the Identifying secured 1-hop node phase starts.

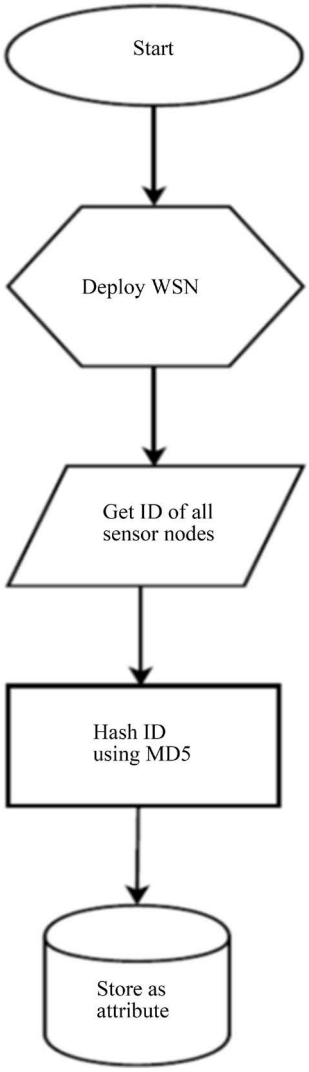

Figure 1. Initialization & set up.

4.2. Identifying Secured 1-Hop Nodes

By identifying secured 1-hop node, malicious nodes are bypassed to join the WSN and only authentic nodes are allowed to join the network at the beginning stage. To authenticate nodes, MD5 algorithm is applied, which provides the hash value of the sensor node ID according to the steps given in the pseudo code of the MD5 algorithm.

After the deployment of the sensor nodes in the network, node A tries to identify its 1-hop nodes. It broadcasts a HELLO message, which consists of its ID (ID_A), it Geographic Location (GL_A) and a Hash Value Attribute (HVA_A) and then waits for each 1-hop neighbour node B to respond.

$$A \rightarrow *: \text{HELLO}\ (ID_A, GL_A, HVA_A). \tag{1}$$

Node B verifies and responds to A by sending a message that consists of its ID (ID_B), its Geographic Location (GL_B) and an authenticator V_B calculated as $H(ID_B)$

$$B \rightarrow A: (ID_B, GL_B, V_B). \tag{2}$$

Upon receiving this message, node A starts to compute the verifier as V'_B.

$$V'_B = \text{Stored HVA}\ (ID_B). \tag{3}$$

The verification is successful if and only if the computed hash value for ID_B is equal to the stored hash value of node B. After verifying the equality of V_B & V_B', node A computes the verifier as V_A = H(IDA) and sends valid response to node B and add node B into its secured 1-hop neighbour list.

$$A \rightarrow B : (ID_A V_A). \quad (4)$$

Using similar approach as node A, node B verifies if node A is an authentic 1-hop node and established a secure route and adds it to its secured 1-hop neighbour list as shown in **Figure 2**.

4.3. Routing through Secured 1-Hop Nodes

The Source node initiates and forwards a request to 1-hop intermediate node nearest to the base station among all its 1-hop neighbour nodes. When the intermediate node receives a request for which it has available 1-hop node to transmit, it forwards a request to the next intermediate node or base station. If there is no available next 1-hop node to transmit, it is defined as block situation. To solve this, step back to its previous 1-hop node and mark itself as a block node. From the previous step node tries to find next available 1-hop neighbour node. The step back & mark will be repeatedly executed until it finds a next 1-hop node for greedy forwarding as shown in **Figure 3**. A decreasing order number-based label is given to the found 1-hop node along with the path number.

Once the routing path is found, acknowledgment is sent back from the base station to the source node. Any node with the same path number sends acknowledgement to its 1-hop secured node which is labelled with the same path number and the largest node number. After receiving acknowledgement, the source node initiates the data transmission to the path with the pre-assigned path number. A release command is issued to all the other 1-hop nodes which are not used for transmission.

5. Simulation & Evaluation

Simulation is done and analyzed with wireless sensor network simulator NetTopo. The goal of simulation of GSTP algorithm is to prove that it can find more number of routing path than that of SecuTPGF and can have

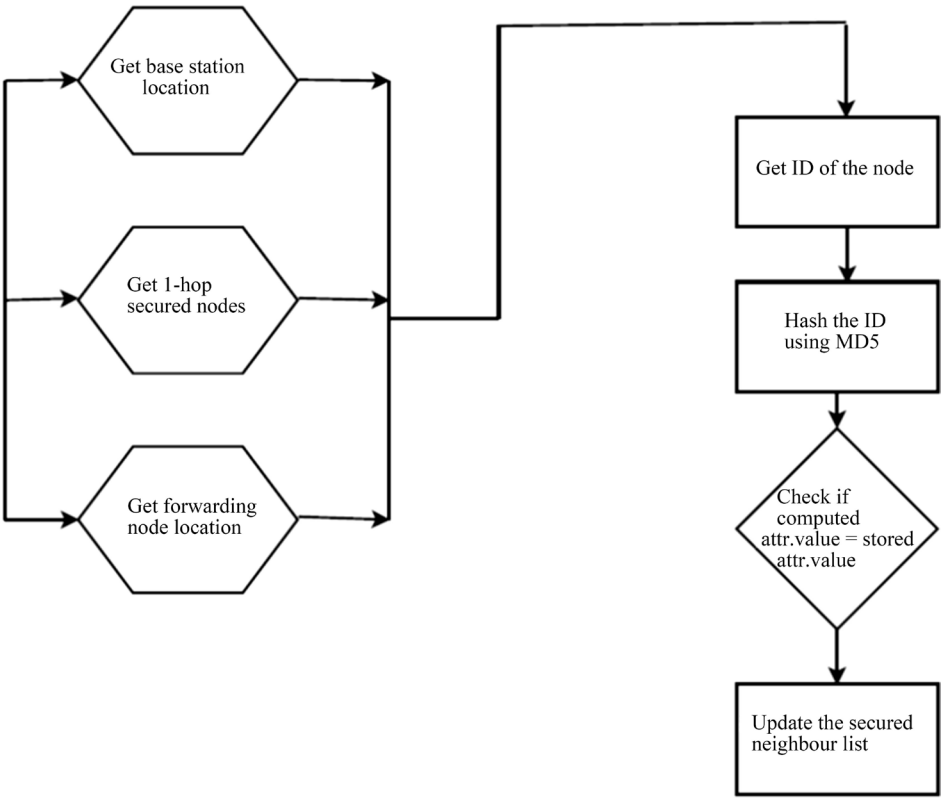

Figure 2. Identifying secured 1-hop nodes.

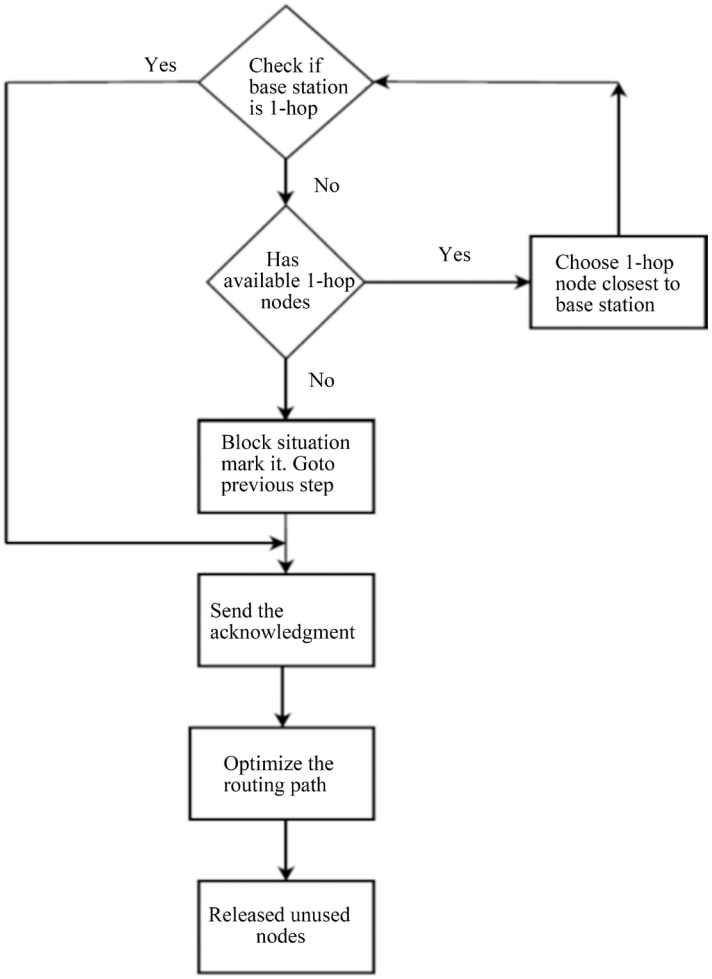

Figure 3. Secured forwarding and routing.

shorter average path length.

The end-to-end delay is defined as: The average delay of each hop is $D_{hop} + D_{otherfactors}$.

$$D_{e2e} = K*\left(D_{hop} + D_{otherfactors}\right) \tag{5}$$

where K is number of hops, D_{hop} is delay in transmission,

$D_{otherfactor}$ is delay with other factors.

For each hop ($D_{hop} + D_{otherfactors}$) the average delay is fixed value.

$$\text{Therefore} \quad D_{e2e} \alpha\ K\ . \tag{6}$$

From Equation (6), the end-to-end delay is directly proportional to the number of hops, K. If the number of hops is less, the end-to-end delay that is the time taken to transmit the information is also reduced.

Routing algorithms have used many routing metrics to determine the best route. Most of the sophisticated algorithms use multiple metrics, where it is combined into a single metric to determine the best route. Some of the metrics used are:

1) Path length is the most common metric. It is defined as the sum of the costs associated with each link visited. Some protocols use hop count, a metric that indicates the number of intermediate nodes that a packet must pass through from a source node to a sink node.

$$P_{Length} = K\left(\text{Number of Hops}\right). \tag{7}$$

2) Routing Delay or End to End delay is also another common metric. It refers to the length of the time re-

quired to transmit the information from the source node to the sink node. From Equation (6) End to End delay can be computed.

To evaluate the GSTP routing algorithm, the simulation network size is fixed as 640 × 400. The average number of hops and the average number of paths are computed by changing the node number (From 100 to 1000) to obtain different values.

Table 1 shows the simulation parameters used for the simulation. Maximum transmission radius is the important parameter that affects the amount of information received at the base station. **Table 2** shows the comparison simulation results of Average number of hops computed before and after optimisation in finding the routing paths using SecuTPGF and GSTP Algorithms.

Figure 4 & **Figure 5** show the simulation results on the average number of hops with 25% malicious nodes that is found by applying GSTP and SecuTPGF respectively. MD5 algorithm retrieves the hash value present in the base station. After retrieving a local hash value present in the forwarding node, if the difference is found between the local hash value and the value found in the base station, it will result in a different hash. It is considered as malicious node. This process affirms an end-to-end delay authentication security for the entire period of transmission. As the security feature is much concentrated, it minimises the average of hops. By comparing the average number of hops in the given figure, it is observed that GSTP routing having less number of hops than that of SecuTPGF.

Table 3 shows the comparison simulation results of number of routing paths computed using SecuTPGF and GSTP Algorithms.

Figure 6 is the simulation results on average number of paths. Basically SecuTPGF is a multipath routing algorithm, Multipath routing refers to a routing strategy that finds more than one path to the destination according to certain constraints. These paths share the network load, aiming at routing efficiency. By comparing the results in the given figure, can easily see that GSTP routing can find much more number of paths than that of SecuTPGF when the number of nodes is more than 500 nodes.

Table 1. Simulation parameters.

Parameter	Value
Network size	640 × 400 m
Number of sensor nodes	100 - 1000
Number of base station	1
Number of source nodes	1
Initial Energy of sensor nodes	10 J
Transmission radius	60-120
Maximum rate	10
Expected life time	1 - 14 Hrs

Table 2. Average number of hops.

No. of nodes	Before optimization		After optimization	
	GSTP	SecuTPGF	GSTP	SecuTPGF
100	17	0	12	0
200	18	23	13	18
300	17	24	14	17
400	14	22	12	17
500	14	20	12	16
600	14	19	12	16
700	16	18	12	16
800	17	18	11	16
900	21	20	10	15
1000	21	19	11	15

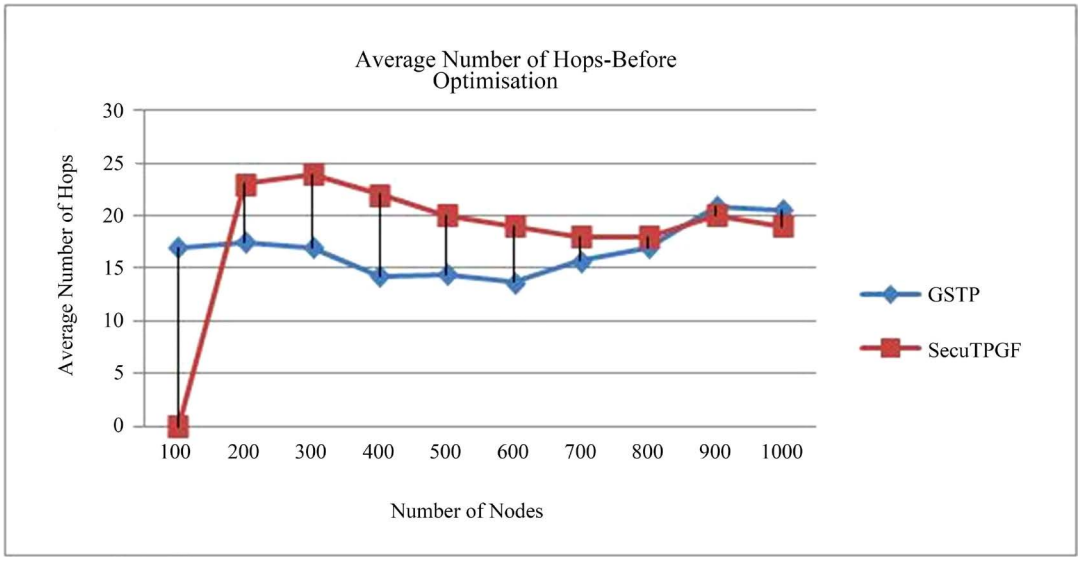

Figure 4. Average number of hops—before optimization.

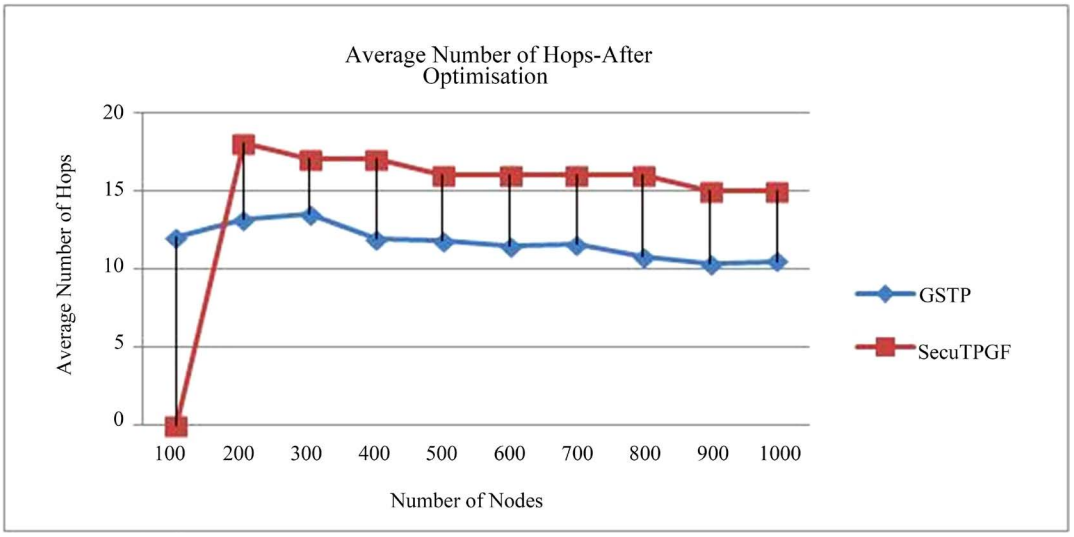

Figure 5. Average number of hops—after optimization.

Table 3. Number of paths identified.

No. of nodes	GSTP	SecuTPGF
100	1	0
200	6	23
300	10	24
400	12	22
500	19	20
600	22	19
700	29	19
800	35	18
900	36	20
1000	44	19

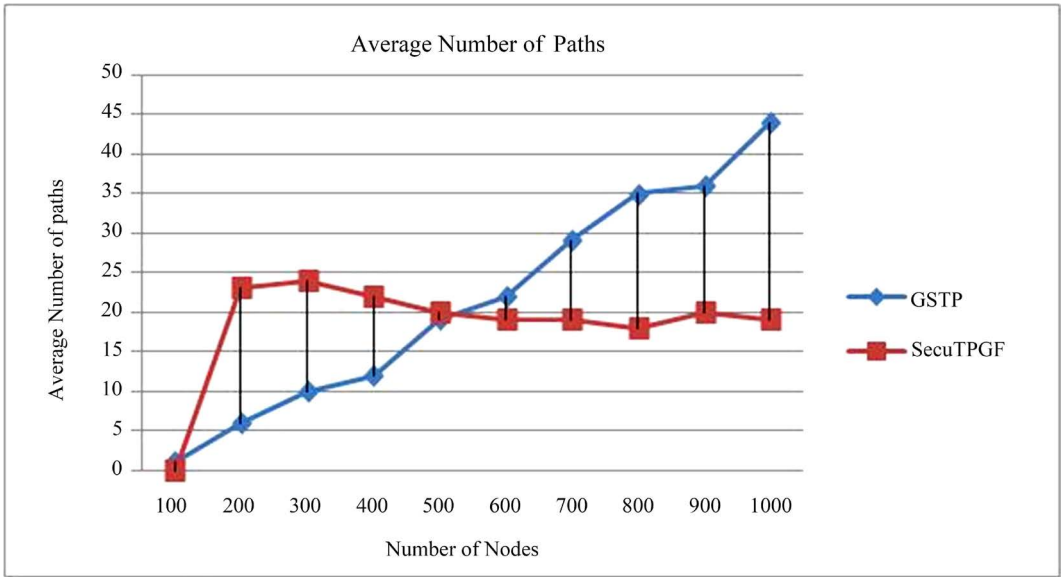

Figure 6. Average number of paths.

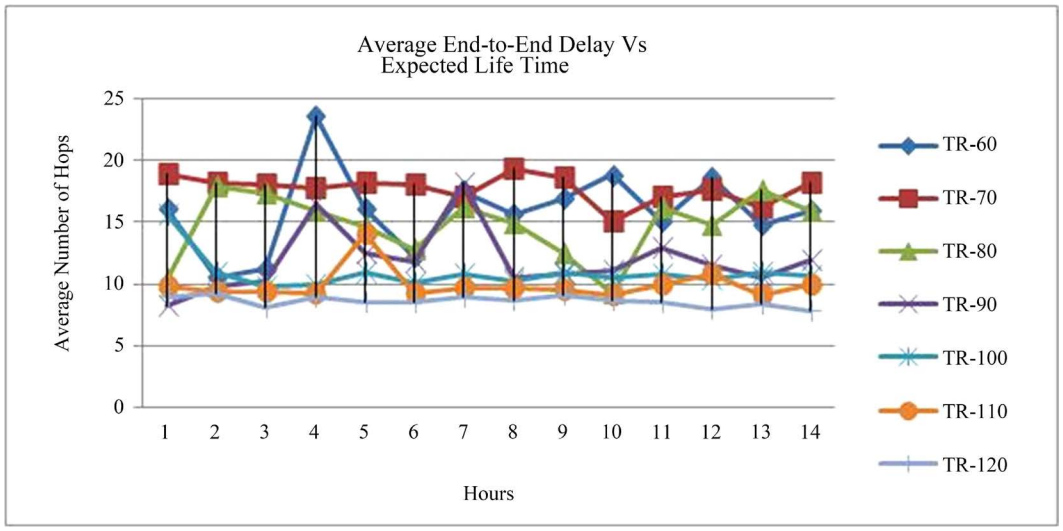

Figure 7. Average end-to-end delay vs expected life time.

Figure 7 is the simulation results on average end-to-end delay over an expected life time. By comparing the results given in the figure, it is observed that there is a significant decrease in the average number of hops as the Transmission Radius is increased for a fixed number of nodes and area. Here the number of nodes taken for the simulation is 500 nodes and the transmission radius is varied from 60 to 120 m. When the transmission radius is 120 m, the number of hops used to transmit the data is reduced.

6. Demonstration and Comparison of SecuTPGF and GSTP

In this section, the snapshots of the execution results of both SecuTPGF and GSTP in NetTopo are given. The Blue colour nodes are normal nodes and Pink colour nodes are malicious nodes,

6.1. Identifying Secured 1-Hop Nodes

Figure 8 shows the network connectivity, in which the malicious nodes are not included in the secured neighbour list. MD5 algorithm verifies the stored hash value with the locally generated hash value present in the

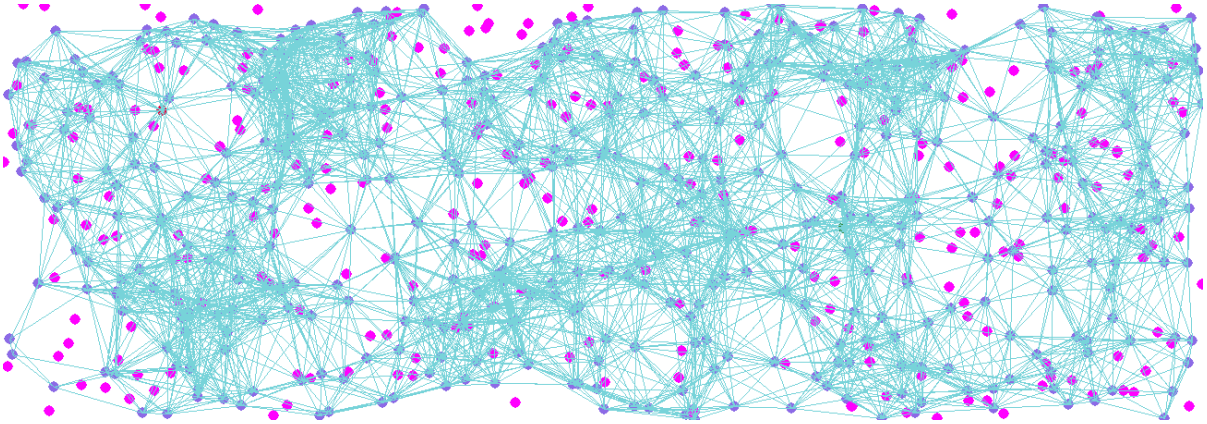

Figure 8. Network connectivity—malicious nodes excluded in secure neighbour list.

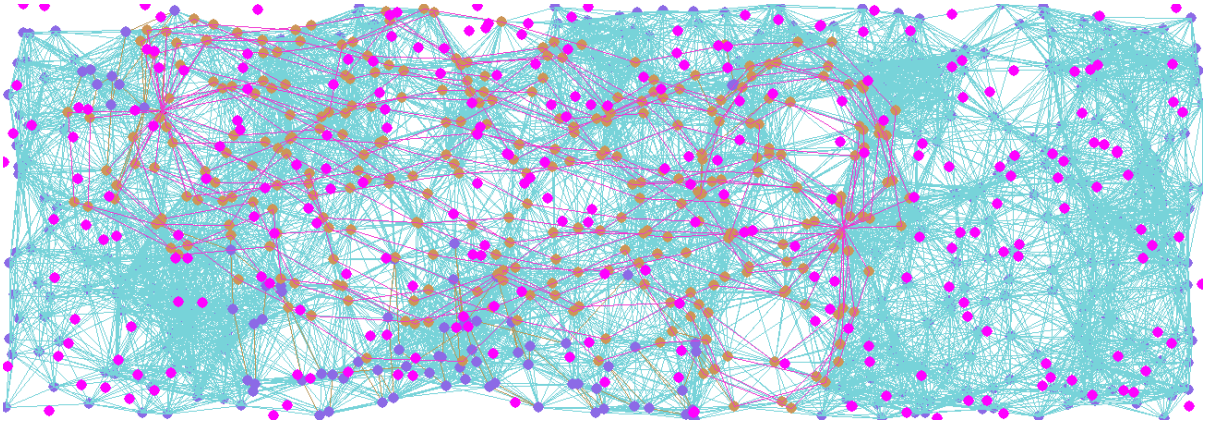

Figure 9. GSTP routing—malicious nodes are excluded in transmission path.

forwarding node. If it matches, that node is considered as a secured node and added to the secured neighbour list.

6.2. Routing through Secured 1-Hop Nodes

Figure 9 shows the execution of GSTP in NetTopo in which malicious nodes are not included in the transmission paths. When the intermediate nodes receive a route request, it checks whether the base station is in 1-hop, if it is, it builds up the route and sends the acknowledgment. If it is an intermediate 1-hop node, it simply forwards it to the next secured 1-hop node. This is repeated until the base station is reached.

7. Conclusion and Future Work

In this paper, the proposed GSTP exactly follows the original SecuTPGF protocol's routing mechanisms and applies MD5 algorithm to provide both the node and message authentication which allows it to secure the identification of 1-hop node and routing through 1-hop node. The work has also analysed and simulated with the values assigned to parameters on system performance. Results achieved prove that GSTP routing using MD5 yields good performance on secured routing using MD5 hashing algorithm. Proposed GSTP algorithm produces good results for varying node density.

In future work, GSTP routing can be sleep scheduled for energy conservation and various attacks for sleep scheduling algorithms need to be considered.

References

[1] Shu, L., Zhang, Y., Yang, L.T., Wang, Y., Hauswirth, M. and Xiong, N.X. (2010) TPGF: Geographic Routing in

Wireless Multimedia Sensor Networks. *Telecommunication Systems*, **44**, 79-95.

[2] Mulugeta, T., Shu, L., Hauswirth, M., Chen, M., Hara, T. and Nishio, S. (2010) Secure Two Phase Geographic Forwarding Routing Protocol in Wireless Multimedia Sensor Networks. *IEEE Transactions on Information Theory*, **22**, 644-654.

[3] Khemapech, I., Miller, A. and Duncan, I. (2005) Simulating Wireless Sensor Networks. Technical Reports, School of Computer Science, University of St Andrews.

[4] Shu, L., Zhang, Y., Zhou, Z., Hauswirth, M., Yu, Z. and Hynes, G. (2008) Transmitting and Gathering Streaming Data in Wireless Multimedia Sensor Networks within Expected Network Lifetime. *ACM/Springer Mobile Networks and Applications* (*MONET*), **13**, 306-322.

[5] Shu, L., Wu, C. and Hauswirth, M. (2008) NetTopo: Beyond Simulator and Visualizer for Wireless Sensor Networks. Technical Report of Digital Enterprise Research Institute, July, 2008.

[6] Shu, L., Hauswirth, M., Chao, H.-C., Chen, M. and Zhang, Y. (2011) NetTopo: A Framework of Simulation and Visualization for Wireless Sensor Networks. *Ad Hoc Networks*, **9**, 799-820. http://dx.doi.org/10.1016/j.adhoc.2010.09.003

[7] Kakkar, A., Singh, M.L. and Bansal, P.K. (2012) Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network. *International Journal of Engineering and Technology*, **2**, 87-92.

[8] Eswar Rao, K. and Naresh Kumar, K. (2012) Performance Analysis of Routing Metrics for Wireless Sensor Networks. *International Journal of Modern Engineering Research*, **2**, 4128-4132.

[9] Guerrero-Zapata, M., Zilan, R., Barcel-Ordinas, J., Bicakci, K. and Tavli, B. (2010) The Future of Security in Wireless Multimedia Sensor Networks. *Telecommunication Systems*, **45**, 77-91.