Journal of Engineering Science and Technology
Vol. 12, No. 2 (2017) 518 - 529

A NOVEL RESOURCE CONSTRAINT SECURE(RCS) ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

R. GEETHA[1,*], E. KANNAN[2]

[1]Department of Computer Science and Engineering, S.A.Engineering College, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
[2]School of Computing and Information Technology, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology Chennai, India
*Corresponding Author: geetha111@yahoo.com

Abstract

Geographic routing protocols are the most preferred routing protocols for Wireless Sensor Networks (WSN) since they rely on geographic position information. Hence we propose geography based Resource Constraint Secure routing (RCS) protocol. The existing routing protocol named Cost Aware SEcure Routing (CASER) allows messages to be transmitted using random walking routing strategy. In the Random walking method, there is a chance of choosing low energy node as a relay node. RCS protocol overcomes this by transmitting the data via energy aware route only and it provides authentication by using Modified ElGammal Signature (MES) scheme on Elliptic curve algorithm. For security purposes, the content of each message can also be encrypted by using a symmetric key encryption technique and decoded at the sink node by knowing the same secret key used by the source. So, unauthenticated person cannot access the original data. Therefore the protocol ensures a secure message delivery option to maximize the message delivery ratio under adversarial attacks. The performance evaluation results show that RCS performs better than CASER with respect to Packet Delivery Ratio, Energy Balance Factor and End-to-End Delay, Throughput and Routing overhead.

Keywords: Random walking, Wireless sensor networks (WSN), Routing, security.

1. Introduction

Wireless Sensor Network (WSN) is used in different applications ranging from military to civilian applications including monitoring environmental conditions. WSN consists of a collection of large number of small devices randomly deployed

Nomenclatures

dg	Destination Grid
G	Base point on the elliptic curve
gh	Grid head
h	Hash function
k_A	Random integer
M	A message to be signed
sg	Source grid
Th	Threshold

Abbreviations

CASER	Cost Aware SEcure Routing
ECC	Elliptic Curve Cryptography
GHT	Geographic Hash Table
GPSR	Greedy Perimeter Stateless Routing
MES	Modified Elgammal Signature
SHA	Secure Hash Algorithm
WSN	Wireless Sensor Network

with non-replinishable energy resources. Because of this limitation, routing in wireless sensor networks is a great challenge. Routing is challenging in wireless sensor networks since it cannot provide high message delivery ratio with little energy consumption [1]. Routing protocols must ensure uniform energy consumption and provide secure routing among the sensor nodes thereby extending the sensor network lifetime [2]. Inspite of the aforementioned issues, since wireless sensor networks rely on wireless communication it can be easily attacked by the adversaries due to the open physical boundary of the network. Since the adversaries are well equipped they can perform malicious activities over the network such as jamming and trace-back attacks [3].

Wireless devices have a restricted transmission range for multi-hop communications, which becomes a real constraint when it exceeds the transmission range of nodes. WSNs represent an example of wireless networks that are emerging as latest trends among researches today because of their budding usages. A sensor network is defined as the constitution of a large number of nodes. The nodes of the network, referred to as sensor nodes, are battery-operated compact devices with the non-renewable energy resources. These sensors are normally deployed with uniform energy among them. But when it comes to the two divergent design issues for multi-hop wireless sensor networks, it relies on the energy balance and security.

Since all the nodes have non-rechargeable batteries so that the nodes die due to loss of energy, so lifetime optimization becomes a major issue while designing the network. Lifetime of the network mainly focuses on the message delivery ratio of the data packets among the sensor nodes. A large number of routing algorithms for WSNs have been emerged but most of them do not take into consideration the limited energy resources for sensor nodes. This is a main pitfall in major routing algorithms, where the routes are not selected based on the energy availability of nodes. This will not protract the lifetime of the sensor nodes and thus the network. There are various Topology-control algorithms including large amount of non-geographic ad hoc routing protocols proposed that are either proactive (maintain

routes continuously) or reactive (create routes on-demand) while reducing energy consumption and improving the security levels of the network.

Nowadays, geographic routing protocols are widely used because they require only local information and thus are very efficacy in wireless networks. Initially, nodes need to know only the location information of the sensor nodes which are in the direct communication range to produce an efficient route towards the sink node. Energy efficient routes are established based on the available power in the nodes or the energy required for transmission in the links across the routes. Next, such protocols preserve both energy and bandwidth since finding floods and propagation of states are not required further on a single hop.

Finally, in wireless networks with frequently changing topology, geographic routing has fast counter and can provide new routes very soon by using local topology information alone [4]. Greedy Perimeter Stateless Routing (GPSR) is one of the familiar geographic routing algorithms that are suggested using face routing to route around barriers when greedy forwarding is unsuccessful. Geographic Hash Tables (GHT) was proved to be successful for sensor networks, and uses a geographic hash table method to store the key-value pair at the sensor node nearest to the hash of the key.

The security issues can be confronted by analyzing the location information in the networks. They analyzed the security attack, as the malicious node does not forward any or part of the received packets. There are various algorithms addressing these security issues in wireless sensor networks such as RSA. The CASER protocol allows messages to be transmitted using two routing strategies, random walking and deterministic routing, in the same framework [5]. The distribution of these two strategies is determined by the specific security requirements. The protocol also provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. They also give quantitative secure analysis on the CASER protocol. Source location Privacy is another major issue to be addressed in WSN [6]. But the main disadvantage of CASER is that it uses random walking to create routing path uncertain for source location privacy [7] and prevention of adversaries attacks [8]. In random walk routing, there is a possibility for the relay node to select the low energy node as a relay node. This makes the possibility of using the lowest energy node routing and the energy of that specific node is drained and its lifetime reduces. In addition to the random walk the existing routing protocol also relies on flooding.

2. Related Work

Zhang and Shen [9] performed investigation over the unbalanced energy consumption for homogeneously deployed data gathering sensor networks. The authors have considered the network as a division of multiple radiance zones wherein each node has the ability to perform data aggregation. Finally they have proposed a localized zone-based routing protocol which balances the energy consumption between the nodes within each radiance.

Li and Ren [10, 11] developed a two-phase routing algorithm which provides the message confidentiality and source location Privacy. Initially the message is forwarded to a randomly chosen intermediate node in the sensor field before it is

being forwarded to a network integration ring where the messages from diverse directions are mixed. Finally the message is forwarded from the network ring to the sink node.

Xinxiang et al. [12] proposed a novel routing algebra system to investigate the compatibilities between routing metrics and three geographic routing protocols including greedy, face, and combined greedy-face routing. Five important algebraic properties, respectively, named odd symmetry, transitivity, strict order, source independence, and local minimum freeness, are defined in this algebra system. Based on these algebraic properties, the necessary and sufficient conditions for loop-free, delivery-guaranteed, and consistent routing are derived when greedy, face, and combined greedy-face routing serve as packet forwarding schemes or as path discovery algorithms, respectively.

Tsui et al. [13] aimed to address the lack of a joint routing-and-sleep-scheduling scheme in the literature by incorporating the design of the two components into one optimization framework. Notably, joint routing-and sleep-scheduling by itself is a non-convex optimization problem, which is difficult to solve. The work tackles the problem by transforming it into an equivalent Signomial Program (SP) through relaxing the flow conservation constraints. The SP problem is then solved by an Iterative Geometric Programming (IGP) method, yielding a near optimal routing-and-sleep-scheduling scheme that maximizes network lifetime. The near optimal solution provided by this work opens up new possibilities for designing practical and heuristic schemes targeting the same problem, for now the performance of any new heuristics can be easily evaluated by using the proposed near optimal scheme as a benchmark.

Li et al. [14] proposed a scalable authentication scheme based on Elliptic Curve Cryptography (ECC). While enabling intermediate node authentication, the proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, the scheme can also provide message source privacy. Both theoretical analysis and simulation results demonstrate that the proposed scheme is more efficient than the polynomial-based approach in terms of communication and computational overhead under comparable security levels while providing message source privacy.

3. RCS Routing Protocol

Driven by the fact that WSN routing is most often geography based, we propose geography based efficient Resource Constraint Secure routing protocol for WSNs without relying on the concept of flooding. In CASER the messages are transmitted using random walking routing strategy which directs the chance of choosing the nodes with low energy as relay nodes at times. To keep away from this, the data is transmitted via energy aware route only and the MES scheme on Elliptic curve algorithm is used to afford authentication. Elliptic curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. For the sake of security the message content is encrypted using a secret key encryption technique and decrypted at the sink node by knowing the same secret key used by the source. Since the unauthenticated person cannot access the original data, the

protocol provides a secure message delivery opportunity to increase the message delivery ratio in the presence of attacks.

RCS routing protocol ensures balanced energy consumption and secure routing. Also, routing trace-back attacks and hostile traffic jamming attacks can be prevented. The main objective of RCS routing protocol is to provide energy aware and secure routing for message in a wireless sensor network with fixed nodes and to increase the lifetime of network. Our work uses the energy efficient routing and also provides the hop-by-hop security by using the MES Scheme. Our work does not make use of the random walking technique of routing which is being used in the CASER. Since, the random walking technique is not being used in RCS routing protocol, there is no chance of choosing the low energy node as relay node and hence the energy balance of the whole network can be maintained. The authentication is being done using the Modified ElGammal Signature scheme. Along with this signature the security for data packet is provided to detect the adversaries. The message receiver should be able to verify whether the message sent by the authorized node and also verify whether the message has been modified by the adversaries. Every forwarder can verify the message is authenticated or not. In this scheme, the authentication of the message is checked during each and every hop and therefore the security process is a bit complicated.

The mechanism of the proposed routing protocol is explained in Fig. 1. In RCS the network is divided into many grids where in each grid is governed by a Grid Head (*gh*). The GH is selected based on the residual energy of the nodes in the network. The node which is having the highest residual energy within the grid is chosen as the GH of the corresponding grid. In this routing protocol the source grid identifies the destination grid as follows. Source grid(*sg*) forwards the message sent by its member to one of its neighboring grid(*ng*). The GH which is closer to the destination grid (*ddg*) and whose residual energy *(ghre*) is greater than the rest of the GHs is chosen as the neighboring grid. This information is appended to the Shortest Route (*sr*). Message authentication between the Grid Heads is performed by Signature Generation and Verification. The process is continued until the destination grid (*dg*) is reached.

The GHs are periodically re-elected based on their residual energy level and the Threshold (*th*) value. Threshold is the constraint which is enforced in the grid head selection which is nothing but the average residual energy of all the nodes within the grid at a given point of time. This feature of GH selection leads to the maximization of the sensor network lifetime.

//Grid to Grid Message Authentication

//Signature Generation

1. For source grid *sg* to sign the message *m* which is to be sent to the destination grid *dg* it has to follow the below steps.
2. Select a random integer k_A, where $1 \leq k_A \leq N-1$ where N is a very large value.
3. Calculate $r = x_A mod$ N, Where $(sg, dg) = k_A G$.where G is the base point on Elliptic Curve and (sg, dg) are the source and destination grids.
4. Calculate $h_A \overset{l}{\leftarrow} h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and $\overset{l}{\leftarrow}$ denotes the l leftmost bits of the hash. m is the message to be signed.

5. Calculate $s = rd_A h_A + k_A \text{mod N}$ where d_A is the random integer selected by the source grid.
6. If s =0, go back to step 2.
7. The signature is the pair (r, s).

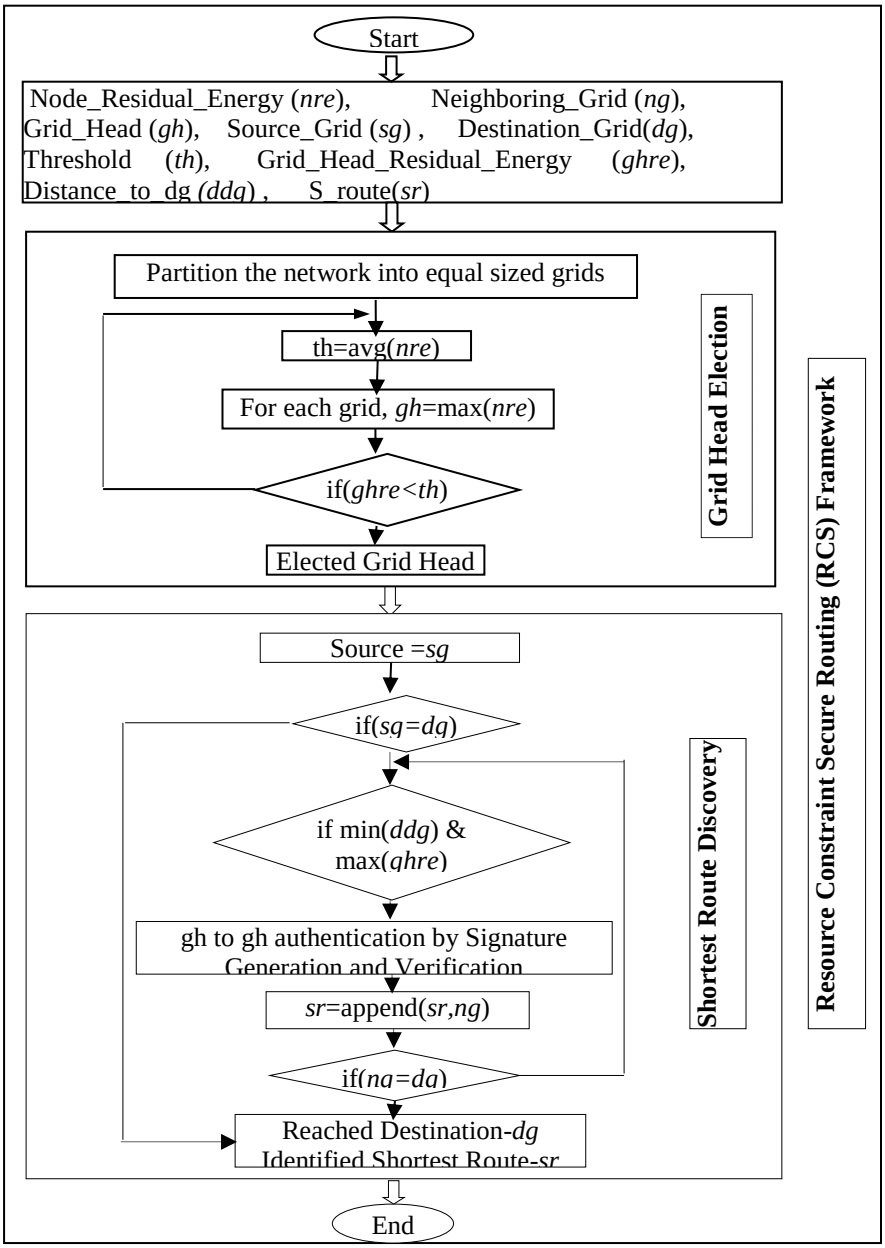

Fig. 1. RCS routing protocol.

//Signature Verification

1. Verify that *r* and *s* are integers in [*1*, *N-1*]. If not, the signature is invalid.
2. Calculate $h_A \overset{l}{\leftarrow} h(m,r)$, where h is the same fucntion used in the signature generation.
3. Calculate (x_1, x_2) = *s G* - r$h_A Q_A$mod *N*.
4. The signature is valid if $r = x_1$ mod *N*, otherwise it is invalid.

RCS protocol gives various advantages facilitating the security and the packet delivery ratio. In random walking there is possibility of choosing low energy node as the relay node. This will lead to flooding problem. The data packets will be sent to the entire nearby grid by verifying its communication range to find the neighboring grids for transmission which will be a threat to adversaries' attacks. Since the RCS sensor nodes periodically update its information to the nearest grids, there will be no delay in delivering the packets to the destination, so the data delivery ratio is being increased. Security is also enhanced by partitioning the network area into grids and manages the nodes inside that particular region. MES scheme on Elliptic curve algorithm used to provide authentication. Symmetric key encryption method is also used to provide authenticated and secure transfer of messages. Modified ElGammal signature is added to the message to be transmitted and if the message is authenticated during the hop, the message is transmitted through deterministic routing strategy to the sink.

4. Performance Evaluation

The performance of RCS protocol against CASER has been evaluated using NS2 simulator since the results can always be matched with the existing original results (both theoretically and experimentally).The comparison results are displayed graphically using the Xgraph in NS2 simulator. In the simulation environment the network has been simulated with 100 nodes with each simulation being repeated twice representing the existing and the proposed works. The three parameters which are being used for comparison are: Packet Delivery Ratio, Energy Balance Factor and End-to-End Delay, Throughput and Routing overhead.

Packet Delivery ratio is used to measure the delivery ratio between CASER and RCS protocols, Energy balance factor is used to compare the energy efficiency of both the factors and End-to-End delay is used to compare the delay ratio between the CASER and RCS protocols. Throughput denotes the rate of successful message delivery. Energy level denotes the overall energy of the network. Routing overhead denotes the resources consumed or lost in the process of communication.

4.1. Packet delivery ratio

Packet Delivery ratio denotes the ratio of actual packet delivered to total packets sent. The packet delivery ratio between the two methods is compared. Fig. 2 shows the comparison of packet delivery ratio between the CASER and RCS routing protocols. The initial linear increase in the graph shows the delivery of packets in both CASER and RCS. And at 4 seconds the graph becomes a straight line, it shows that all the packets have been delivered. Thus, it can be incurred from the graph that the packet delivery ratio of RCS protocol is better than CASER protocol.

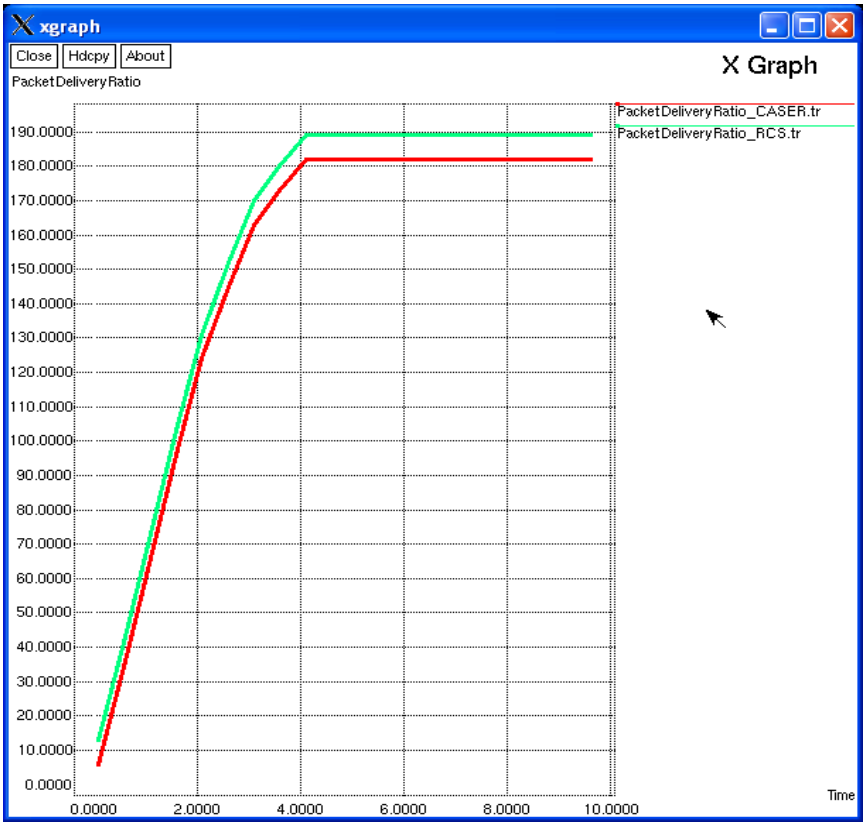

Fig. 2. Packet delivery ratio between CASER and RCS.

4.2. End to end delay

End to end delay denotes the delay that occurs during the transmission of packets between each and every node. The end-to-end delay between the two protocols is compared. Fig. 3 shows the comparison of end-to-end delay between CASER and RCS routing protocol. Since, the CASER protocol uses the technique of random walking; its end-to-end delay is more than that of RCS protocol. Thus, RCS is more delay efficient than CASER protocol.

4.3. Energy balance

Energy balance ratio measures the overall energy remaining after the transmission of messages. The energy balance ratios between two protocols are compared. Fig. 4 shows the initially both the protocols have the same energy. But, as soon as transmission starts, there is a steep decrease in the energy of CASER protocol because the CASER protocol makes use of random walking technique where a low energy node can be used as a relay node and hence decreasing the energy efficiency of the whole network. Thus, RCS protocol offers more energy balance than CASER protocol.

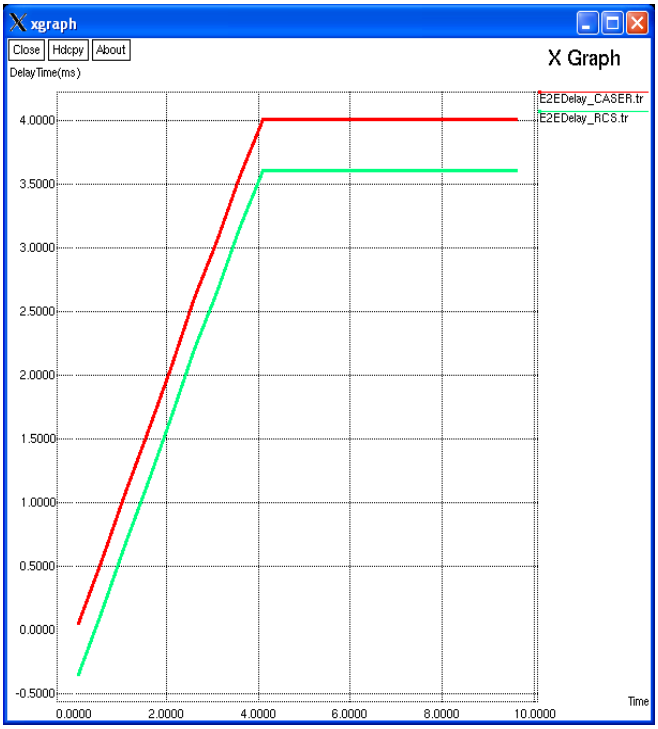

Fig. 3. End-to-End delay between CASER and RCS.

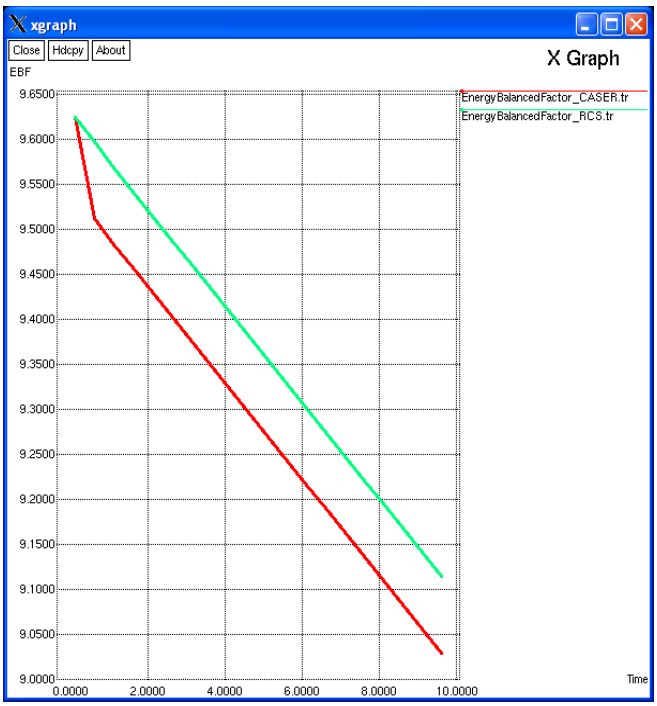

Fig. 4. Energy balance ratio between CASER and RCS.

4.4. Throughput

Throughput denotes the rate of successful message delivery. The throughput between the two protocols is compared. Fig. 5 shows that the throughputs of both the protocols almost coincide since the rate of successful delivery is high in both the protocols. The CASER protocol can have more delay but the rate of successful delivery is high. The straight line after a certain time shows that the complete transmission has occurred and there are no more packets left to transmit.

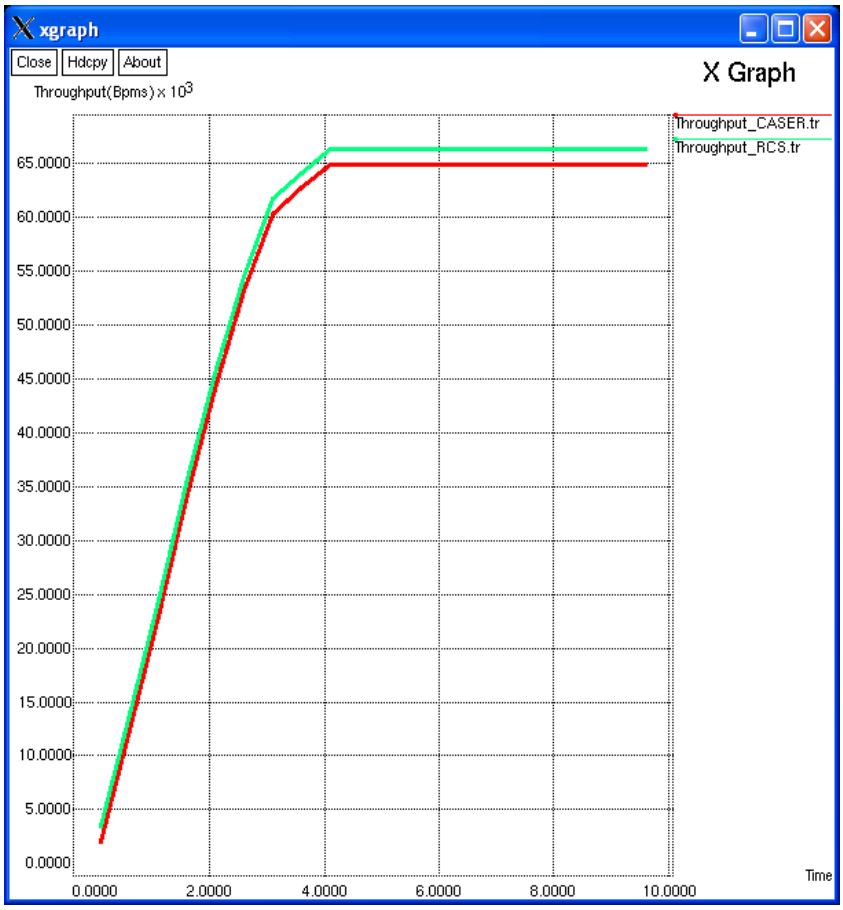

Fig. 5. Throughput ratio between CASER and RCS.

4.5. Routing overhead

Routing overhead denotes the resources consumed or lost in the process of communication. The routing overhead between the protocols is compared. Fig. 6 shows that initially, the routing overhead of CASER is slightly higher due to random walking and after some time it deviates from RCS because of the same. The straight line later shows that the transmission has completed and there is no further overhead.

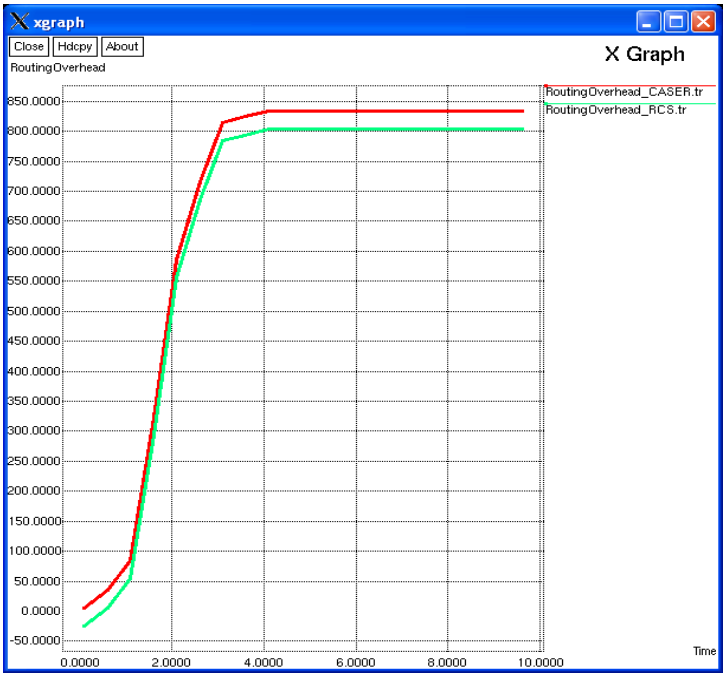

Fig. 6. Routing overhead between CASER and RCS.

5. Conclusion

We have proposed geography based efficient RCS routing protocol for WSNs without relying on flooding. The lifetime optimization of the nodes in the network has been maximized using the proposed routing protocol. RCS combines the technique of deterministic shortest path algorithm with high energy balance ratio. Since the proposed routing protocol does not use random walking technique which is used in CASER protocol, the probability of using the low energy node as relay node decreases. Thus, lifetime of the whole network is increased by the routing protocol which provides high energy optimization, high hop-by-hop authentication of messages and encryption security for transmitted messages. The simulation results show that RCS performs better than CASER with respect to Packet Delivery Ratio, Energy Balance Factor and End-to-End Delay, Throughput and Routing overhead.

References

1. Dargie, W.; and Poellabauer, C. (2010). *Fundamentals of wireless sensor networks: Theory and practice*. Wiley.
2. Hung, C.-C.; Lin, K.C.-J.; Hsu, C.-C.; Chou, C.-F.; and Tu, C.-J. (2010). On enhancing network- lifetime using opportunistic routing in wireless sensor networks. 2010 *Proceedings of 19th International Conference on Computer Communications and Networks* (*ICCCN*), 1-6.
3. Xu, W.; Ma, K.; Trappe, W.; and Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. *IEEE Network*, 20(3), 41-47.

4. Cadger, F.; Curran, K.; Santos, J.; and Moffett, S. (2013). A survey of geographical routing in wireless ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 15(2), 621-653.
5. Tang, D.; Li, T.; Ren, J.; and Wu, J. (2014). Cost-aware SEcure routing (CASER) protocol design for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 26(4), 960-973.
6. Li, Y.; Ren, J.; and Wu; J. (2011). Quantitative measurement and design of source-location privacy schemes for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(7), 1302-1311.
7. Zakhary, S.; Radenkovic, M.; and Benslimane, A. (2014). Efficient location privacy-aware forwarding in opportunistic mobile networks. *IEEE Transactions on Vehicular Technology*, 63(2), 893-906.
8. Pathan, A.S.K.; Lee, H.-W.; and Hong, C.S. (2006). Security in wireless sensor networks: issues and challenges. *Proceeding of the 8th International Conference on Advanced Communication Technology*, 2, 1043.-1048.
9. Zhang, H.; and Shen, H. (2009). Balancing energy consumption to maximize network lifetime in data-gathering sensor networks. *IEEE Transactions on Parallel and Distributed. Systems*, 20(10), 1526-1539.
10. Li, Y.; and Ren, J. (2009). Preserving source-location privacy in wireless sensor networks. *Proceedings of 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 1-9.
11. Li, Y; and Ren, J. (2010). Source-location privacy through dynamic routing in wireless sensor networks. *2010 Proceedings IEEE INFOCOM*, 1-9.
12. Li, Y.; Yang, Y.; and Lu, X. (2010). Rules of designing routing metrics for greedy, face, and combined greedy-face routing. *IEEE Transactions on Mobile Computing*, 9(4), 582-595.
13. Liu, F.; Tsui, C.-Y.; and Zhang, Y.J (2010). Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks. *IEEE Transactions on Wireless Communications*, 9(7), 2258-2267.
14. Li, Y.; Li, J.; Ren, J.; and Wu, J. (2012). Providing hop-by-hop authentication and source privacy in wireless sensor networks. *2012 IEEE INFOCOM*, 3071-3075.