International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

An Energy Efficient Secure Multipath Routing Algorithm for Wireless Sensor Network

R. Sudha[1], C. Nandhini[2]

[1]Assistant Professor, Dept of CS, PSG College of Arts & Science, Coimbatore, Tamilnadu, India

[2]Research scholar, Dept of CS, PSG College of Arts & Science, Coimbatore, Tamilnadu, India

Abstract: ***In Networks messages are transfer through the nodes. When transferring the message, the passing messages will send with the secure mode. Here, low energy nodes are in sleep state and the high energy nodes are in active stage. Whenever the nodes are in sleep state it is enable to monitor the message transfer. For these ways it reduces the power consumption and this system is efficient when the messages are being transmitted. The encryption is done from node to node when transferring the message and after the message reached the destination node the decryption takes place. Here, the security also improved, messages are being transmitted from source to destination.***

Keywords: Sensor networks, CASER, SWSR, RSA, Security

1. Introduction to Computer Network

A computer network or data network is a telecommunications network that allows computers to exchange data. Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. Network computer devices that originate, route and terminate the data are called network nodes.

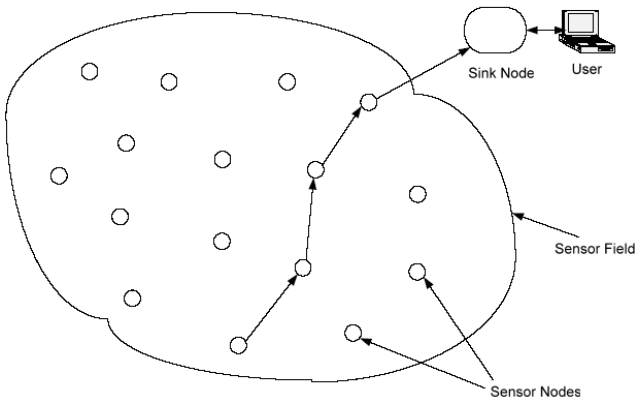
Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

2. Introduction to Wireless Sensor Network

The wireless sensor networks of the near future are envisioned to consist of hundreds to thousands of inexpensive wireless nodes, each with some computational power and sensing capability, operating in an unattended mode. They are intended for a broad range of environmental sensing applications from vehicle tracking to habitat monitoring. The applications, networking principles and protocols for these systems are just beginning to be developed. Sensor networks are quintessentially event-based systems.

A sensor network consists of one or more "sinks" which subscribe to specific data streams by expressing interests or queries. The sensors in the network act as "sources" which detect environmental events and push relevant data to the appropriate subscriber sinks.

The scope of this paper is focused on position-based routing, also called geometric or geographic routing. Position-based routing protocols are based on knowing the location of the destination in the source plus the location of neighbours in each node.



The basic structure of Wireless Sensor Networks

A Wireless Sensor Network is comprised solely of wireless stations. The communication between source and destination nodes may require traversal of multiple hops because of limited radio range. Existing routing algorithms can be broadly classified into topology-based and position-based routing protocols.

Topology-based routing determines a route based on network topology as state information, which needs to be collected globally on demand as in routing protocols DSR and AODV or proactively maintained at nodes as in DSDV.

3. Related Work

3.1 The Existing Work and Problem Definition

CASER protocol has two major advantages: (i) It ensures balanced energy consumption of the entire sensor network so that the lifetime of the WSNs can be maximized. (ii) CASER protocol supports multiple routing strategies based on the routing requirements, including fast/slow message delivery and secure message delivery to prevent routing trace-back attacks and malicious traffic jamming attacks in WSNs.

Previous work proposes a secure and efficient Cost-Aware Secure Routing (CASER) protocol for WSNs. In this protocol, cost-aware based routing strategies can be applied to address the message delivery requirements. We devise a quantitative scheme to balance the energy consumption so that both the sensor network lifetime and the total number of messages that can be delivered are maximized under the same energy deployment. We develop theoretical formulas to estimate the number of routing hops in CASER under varying routing energy balance control and security requirements.

We quantitatively analyze security of the proposed routing algorithm. We provide an optimal non-uniform energy deployment strategy for the given sensor networks based on the energy consumption ratio. Our theoretical and simulation results both show that under the same total energy deployment, we can increase the lifetime and the number of messages that can be delivered more than four times in the non-uniform energy deployment scenario.

Drawbacks

The adversaries will have sufficient energy resources, adequate computational capability and enough memory for data storage. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. They can move to this sender's location without too much delay. They may also compromise some sensor nodes in the network.

- The adversaries will not interfere with the proper functioning of the network, such as modifying messages, altering the routing path, or destroying sensor devices, since such activities can be easily identified. However, the adversaries may carry out passive attacks, such as eavesdropping on the communications.
- The adversaries are able to monitor the traffic in any specific area that is important for them and get all of the transmitted messages in that area. However, we assume that the adversaries are unable to monitor the entire network. In fact, if the adversaries could monitor the entire WSN, they can monitor the events.

In existing the power consumption is high whenever the messaging is transfer. Here, the security for transferring the message is not highly secured. When transferring the message from one node to another node there is a delay and it is unable to monitor the entire node.

4. Proposed Techniques

The proposed research schemes to achieve capacity close to the node to node energy reduction and secure transmission. In addition, though the one dimensional mobility model constrains the direction of nodes' mobility, it achieves larger capacity than the two dimensional model since it is more predictable. Also, slow mobility brings better performance than fast mobility because there are more possible routing schemes called as sleep awake state routing. A variety of mobility models which are also widely adopted in previous works.

Thus, multicast sessions are formed. Our results in homogeneous network are further used to study the heterogeneous network, where $m = n$ base stations connected with wires are uniformly distributed in the unit square. By removing some limitations and constraints, for the present fundamentals. They can give a general analysis on the optimal multicast capacity-delay tradeoffs in both homogeneous and heterogeneous wireless sensor networks. We assume a mobile wireless network that consists of n nodes, among which $ns = ns$ nodes are selected as sources and $nd = n$ destined nodes are chosen for each. The purpose of this paper is to conduct extensive analysis on the multicast capacity-delay trade-off in wireless sensor networks.

Limited by the energy storage capability and security of wireless sensor nodes, it is crucial to jointly consider security and energy efficiency and security in data collection of WSNs. The disconnected multipath routing scheme with secret sharing is widely recognized as one of the effective routing strategies to ensure the safety of information. This kind of scheme transforms each packet into several shares to enhance the security of transmission. Many to many WSNs, shares have high probability to traverse through the same link and to be intercepted by adversaries. In this paper, we formulate the secret-sharing-based multipath routing problem as an optimization problem. Our objective aims at maximizing both network security and lifetime, subject to the energy constraints using sleep wake state routing protocol with RSA Based Security.

4.1 Routing Algorithm

Sleep Wake State Routing Protocol

1. Node *S* broadcasts a wake-up signal to all its first-hop neighbours. The wake-up signal includes the identity of both the current sender (*S*), the next-hop (*n1*), and the previous-hop (empty for *S*).

2. Each neighbour of *S*, after being woken up, decides whether to stay awake or go back to sleep based on the role that it may play on the ongoing communication. If that neighbour is the next-hop (*n1*), it stays awake to forward the data and to monitor the next-hop from it(*n2*). If that neighbour is a guard for the next-hop *n1* over the link *n1*and *n2*, it stays awake to monitor the behaviour of *n1*. If the node is a guard of a forwarding node over the previous-hop, it stays awake to detect fabrication by the forwarding node. A node can independently make this determination based on first and second-hop neighbour information. If none of these cases hold, the node goes back to sleep immediately.

3. Node *S* sends the data packet to *n1* following the timing schedule presented

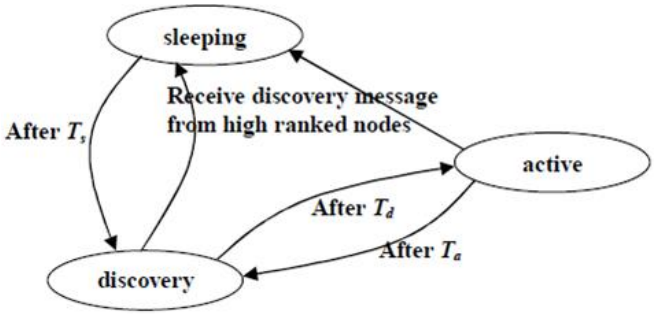
4. Nodes after being woken up continue to stay awake for *Tw*. After that, it goes back to sleep.

5. *n1* does the same steps that *S* did to wake up the next hop(*n2*), *n2*'s guards and *n1*'s guards.

6. If *n1* fails to send the wakeup signal, the guard of *n1*with the lowest ID sends a two-hop broadcast of the Wake up

signal through. If that guard fails, the guard with the next smallest ID sends the signal, and so on. This design ensures that if there is a chain of colluding malicious nodes then all the nodes will be suspected.

7. The process continues at each step till the destination.



Sleep wake state routing protocol

5. Security Techniques

Here RSA aogorthim is used for security purpose.

RSA ALGORITHM

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of a integer is hard for factoring the problem.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

6. Result and Discussion

This analysis includes calculating percentage of energy conserved in this protocol as well as the previously known protocol. Further time spend by each node in the sense, transmit, off states are calculated for each node. Based on the above results, power consumption of each node in their corresponding state is calculated. Total power consumed by a single sensor node is calculated based on the individual power consumed by the corresponding node in the sense, transmit, off states.

	Message Ratio	Delivery Time
Proposed Protocol	98	24
Existing Protocol	40	84

Message vs Time

Total power consumed by a single sensor node is calculated based on the individual power consumed by the corresponding node in the sense, transmit, off states.

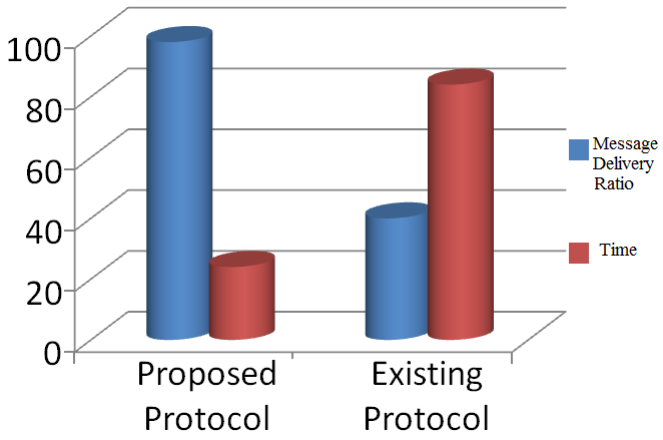


Chart for Message Delivery ratio and Time for Proposed and Existing Protocol

Total power consumption of the entire process is calculated based on the total power consumption of the individual nodes. Finally, percentage of energy conserved in this work and previous work is calculated. Theoretical analysis is performed for both static and mobile events. Theoretical results for static events are shown below:

== Time Spent By Each Node in Sense State ==

Time spent by the node 0:: 49.92739999999999 ms
Time spent by the node 1:: 49.92739999999999 ms
Time spent by the node 3:: 49.87657999999999 ms
Time spent by the node 4:: 50.0 ms
Time spent by the node 5:: 50.0 ms
Time spent by the node 6:: 50.0 ms
Time spent by the node 7:: 50.0 ms
Time spent by the node 8:: 49.91651000000000 ms
Time spent by the node 9:: 49.8765799999999 ms

==Power Consumed By Each Node in Sense State ===

Power consumed by the node 0:: 49.9273999999999999 mW
Power consumed by the node 1:: 49.9273999999999999 mW
Power consumed by the node 3:: 49.7204899999999999 mW
Power consumed by the node 4:: 49.8765799999999999 mW
Power consumed by the node 5:: 50 mW
Power consumed by the node 6:: 50 mW
Power consumed by the node 7:: 50 mW
Power consumed by the node 8:: 49.9165100000000000 mW
Power consumed by the node 0:: 49.8765799999999999 mw

7. Conclusion and Future Scope

This work deals with the efficiency of the process, which runs locally at each sensor node in order to govern its operation. Each sensor node conserves its energy by switching between Sense/Receive (or) off states only until it senses an event in its proximity, after which it enters the transmit state to transmit the event information and also shows that the power saved in each node outperforms the power saved in any other previously known protocols and this work also shows that it is possible to minimize about 51% of the power and maintain 100% coverage and

connectivity. Further, simulation study also proves that it is possible to increase the life time of each sensor network by increasing the number of sensor nodes as well as the security of nodes using RSA algorithm.

The future work includes providing security to the information passed to the base station. This work does provide security for the information passed to the base station. The higher security can be provided to the information which is being transmitted by encrypting it and decrypting it at the base station. The information is encrypted by the sensor node using a shared key (The key that is shared between every sensor node and base station) and only the base station sharing its key can decrypt it. No other sensor nodes or station can decrypt it.

References

[1] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 388–404, 2000.
[2] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Networking*, vol. 10, no. 4, pp. 477–486, 2002.
[3] M. Garetto, P. Giaccone, and E. Leonardi, "Capacity scaling in delay tolerant networks with heterogeneous mobile nodes," in *ACM MobiHoc 2007*, New York, USA, 2007, pp. 41–50.
[4] B. Liu, Z. Liu, and D. Towsley, "On the capacity of hybrid wireless networks," in *IEEE Infocom 2003*, vol. 2, San Francisco, USA, 2003, pp. 1543–1552.
[5] U. C. Kozat and L. Tassiulas, "Throughput capacity of random ad hoc networks with infrastructure support," in *ACM MobiCom 2003*, New York, USA, 2003, pp. 55–65.
[6] A. Agarwal and P. R. Kumar, "Capacity bounds for ad hoc and hybrid wireless networks," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 3, pp. 71–81, 2004.
[7] X.-Y. Li, "Multicast capacity of wireless ad hoc networks," *IEEE/ACM Trans. Networking*, vol. 17, no. 3, pp. 950–961, 2009.
[8] X.-Y. Li, Y. Liu, S. Li, and S. Tang, "Multicast capacity of wireless ad hoc networks under gaussian channel model," *IEEE/ACM Trans. Networking*, vol. 18, no. 4, pp. 1145–1157, 2010.
[9] X. Mao, X.-Y. Li, and S. Tang, "Multicast capacity for hybrid wireless networks," in *ACM MobiHoc 2008*, Hong Kong, China, 2008, pp. 189–198.
[10] X.-Y. Li, X. Mao, and S. Tang, "Closing the gap of multicast capacity for hybrid wireless networks," 2009, [Online]. Available: http://www.cs.iit.edu/ xli.
[11] W. Huang, X. Wang, and Q. Zhang, "Capacity scaling in mobile wireless ad hoc network with infrastructure support," in *IEEE ICDCS, 2010*, Genoa, Italy, 2010, pp. 848–857.
[12] M. J. Neely and E. Modiano, "Capacity and delay tradeoff for ad hoc mobile networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1917–1937, 2005.
[13] Y. Guo, F. Hong, Z, Jin, Y. He, Y. Feng and Y. Liu, "Perpendicular Intersection: Locating Wireless Sensors with Mobile Beacon," *IEEE Trans. Vehicular Technology*, vol. 59, no. 7, pp. 3501–3509, 2010.

Author Profile

R. Sudha , Assistant Professor, Dept of CS, PSG college of Arts & Science, Coimbatore, Tamilnadu

C. Nandhini , Research scholar, Dept of CS, PSG college of Arts & Science, Coimbatore, Tamilnadu