ISSN No: 2454-9614

CASER Protocol Enhancing Fake Content Delivery for Trace back Attack Avoidance in WSNs

R. Keerthana[a], J. Jeyaram[a*]

[a)] Department Of Computer Science and Engineering, Vivekananda institute of engineering and technology for women,
Tiruchengode , Tamilnadu, India.
[b)] Department Of Computer Science and Engineering, Vivekananda institute of engineering and technology for women,
Tiruchengode,, Tamilnadu, India.

*Corresponding Author: R. Keerthana

E-mail: keerthanacse048@gmail.com,

Received: 16/11/2015, Revised: 16/12/2015 and Accepted: 6/03/2016

Abstract

Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-replenish able energy resources. A novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic based random walking. The energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To solve this problem, an efficient non-uniform energy deployment strategy used to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. An quantitative security analysis on the proposed routing protocol. The theoretical analysis results demonstrate that the proposed CASER protocol can provide an excellent trade-off between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, shows that increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. CASER protocol also demonstrates can achieve a high message delivery ratio while preventing routing trace back attacks.

Keywords: Routing, Security, Energy Balance, Energy Efficiency.
Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network (WSAN)) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

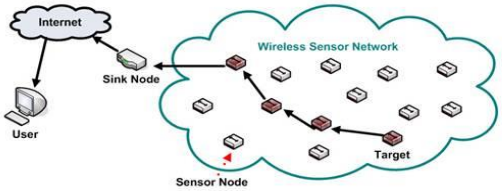


Fig. 1 wireless sensor networks

1.1 Routing Protocols In WSNs

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbours, and then throughout the network. This way, routers gain knowledge of the topology of the network. Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements. Many routing algorithms were developed for wireless networks in general.

1.2 The Adversarial Model

In WSNs, the adversary may try to recover the message source or jam the message from being delivered to the sink node. The adversaries would try their best to equip themselves with advanced equipment's, which means they would have some technical advantages over the sensor nodes.

- 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, 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 directly without relying on other people's sensor network.

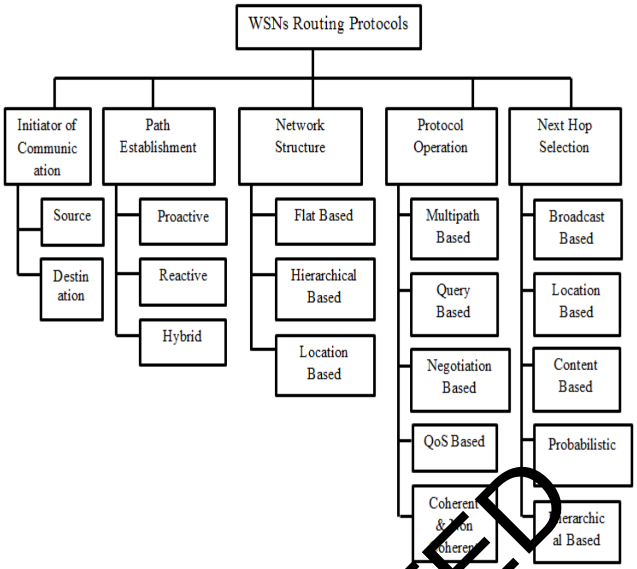


Fig.2 Routing Protocol in WSNs

1.3 Security Goals In WSNs

A wireless sensor network shares some common features with the traditional network and also has unique features of its own that distinguishes it from the traditional network. Therefore, the security goals or requirements cover both the traditional network goals and the goals suited solely to the wireless sensor network. *Confidentiality* is the means of limiting information access to only the authorized users and preventing access or disclosure by the unauthorized users. Data confidentiality is the most important issue that any network must address. If sensor nodes are not capable of keeping the data confidential, then any neighbouring node can tamper with the data and transmit false information. This can cause serious hazards, especially in military applications. *Data authentication* is the ability of a receiver to verify that the data received by it is from a correct sender. In a wireless sensor network, data can not only be tampered by the malicious nodes but the entire packet stream can be changed by addition of false packets to it. Data authentication can be achieved using symmetric key cryptography where the sender and receiver share a secret key or using asymmetric key cryptography where the data can be encrypted and decrypted using public and private keys.

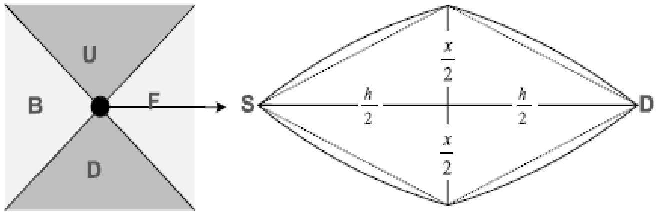
Data Availability determines if the services of the network are available in case of failure or presence of attacks in the network. A single point failure in the network can threaten the availability of resources and other services. So, data availability is of prime importance and is responsible for the operation of the network. *Data Integrity* ensures that the received data is not altered in transit. It confirms that the data is reliable and has not been altered or changed. The network must incorporate security mechanisms against different attacks caused by malicious nodes so as to ensure integrity of the data.

Data Freshness determines that the data is recent and no old packets have been replayed. It is important to ensure the freshness of the message, apart from ensuring data confidentiality and integrity. Weak freshness that provides partial message ordering but doesn't provide any delay information and strong freshness, which provides total message ordering and delay estimation. Weak freshness is used for sensor measurements while strong freshness is employed in time synchronization in the network. *Self-Organization* sensor nodes in a wireless sensor network are randomly deployed and have no fixed infrastructure. So, these sensor nodes must have self-organizing capability so that they can dynamically organize according to the environment and situation. Self-organizing capability is important to ensure multi-hop routing, key management and building trust relations with the neighbors. If self-organizing capability lacks in a sensor network, then damage resulting from attacks can be significant. *Time Synchronization* sensor network applications rely on some form of time synchronization. When a packet travels between two pair wise sensors, sensors can compute the end-to-end delay of a packet. *Secure Organization* utility of a sensor network relies on its ability to accurately and automatically locate each sensor in the network. Wireless sensor networks which are expected to locate faults needs accurate information about a location in order to indicate a fault's location. Unfortunately, a malicious node can manipulate non secured location information by reporting false signal strengths, replaying signals.

2. Dynamic Secure Routing

The network is evenly divided into small grids. Each grid has a relative location based on the grid information. The node in each grid with the highest energy level is selected as the head node or message forwarding. In addition, each node in the grid will maintain its own attributes, including location information remaining energy level of its grid, as well as the attributes of its adjacent neighbouring grids. The information maintained by each sensor node will be updated periodically. We assume that the sensor nodes in its direct neighbouring grids are all within its direct communication range.

We also assume that the whole network is fully connected through multi-hop communications. In addition, through the maintained energy levels of its adjacent neighbouring grids, it can be used to detect and filter out the compromised nodes for active routing selection. The shortest path routing also called deterministic routing, in this routing the next hop grid is selected from the neighbour grid list based on the relative locations of the grid. The grid that is closest to the sink node is selected for message forwarding and also we are considered energy level of the selected node. The selected nodes have the highest energy level when compared with other node's energy levels. In this routing we are using cryptographic technique for message security. The deterministic shortest path routing guarantees that the messages are sent from the source node to the sink node. This routing is also called random walking, in this routing the next hop grid randomly selected from neighbour grid list for message forwarding.



(a) Next hop node distribution

(b) Routing path

Fig.3 Routing path and length

The routing path becomes more dynamic and unpredictable. In this way, it is more difficult for the adversary to capture the message or to jam the traffic. Therefore, the delivery ratio can be increased in a hostile environment. Using this routing we can avoid the jamming. For this we used Cost Aware Secure Routing Protocol. CASER routing strategy that can provide routing path unpredictability and security.

A simple Procedure for the process as follow: Create the nodes and set the communication range for all nodes. Find the neighbour node for the entire node, select the neighbour node based on the communication range, and then calculate the distance from one node another Make the cluster formation. First we need to evenly divide the network area and calculate the energy level for all other nodes, select the highest energy node as a cluster head then select the cluster members and cluster head collects the information from cluster members.

Finally cluster head transmit collected information to the sink. The sensor network lifetime increase through balanced energy consumption throughout the sensor network. In addition, the maintained energy levels of its adjacent neighbouring grids can be used to detect and filter out the compromised nodes for active routing selection. Dynamic routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions.

The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change. People using a transport system can display dynamic routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination. Another example of dynamic routing can be seen within financial markets. For example, ASOR or Adaptive Smart Order Router (developed by Quod Financial), takes routing decisions dynamically and based on real-time market events.

3. Cost Aware Secure Routing Protocol

In CASER routing protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighbouring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design trade-off between security and efficiency. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries. The main focus is on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention.

3.1 System Architecture

The cost-aware based routing strategies can be applied to address the message delivery requirements. 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 (ED).To estimate the number of routing hops in CASER under varying routing energy balance control (EBC) and security requirements.

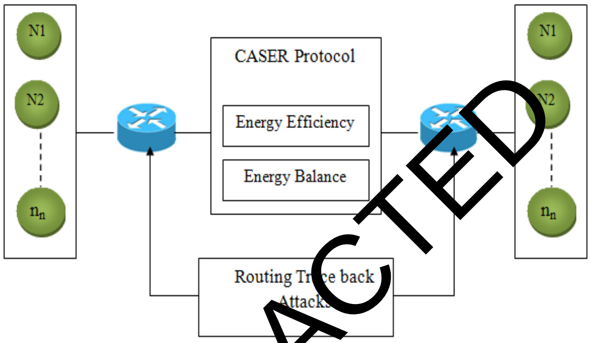


Fig.3 CASER System Architecture

3.2 WSNs File Launching

Create WSNs as needed and start the communication between one to another node. The sender launch the file to the receiver in the network and the receiver will collect the file from the routing. Each network there may some controller/base station which can transfer the file in network with the help of routing protocols. The recent technological advances make wireless sensor networks technically and economically feasible to be widely used in both military and civilian applications. A key feature of such networks is that each network consists of a large number of untethered and unattended sensor nodes. These nodes often have very limited and non-replenish able energy resources which makes energy an important design issue for these network.

3.3 Secure Routing Protocol Design

Wireless sensor domain, anybody with an appropriate wireless receiver can monitor and intercept the sensor network communications.The CASER protocol designed to make the communication without loss or delay on delivery and make the network lifetime to increase and secure. To make the routing more secure the design of CASER has a scheme called dynamic route selection. A properly designed routing protocol should not only ensure high message delivery ratio and low energy consumption for message delivery, but also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime. In addition to the fore mentioned issues, WSNs rely on wireless communications, which is by nature a broadcast medium. It is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary. In particular, in the wireless sensor domain, anybody with appropriate wireless receiver can monitor and intercept the sensor network communications.

3.4 Routing trace back attacks

The routing path becomes dynamic and unpredictable. The message can be sent to the previous node by either of the routing strategies, it is infeasible for the adversary to determine the routing strategy and find out the previous nodes in the routing path. The actual energy is updated periodically. For WSNs with non-replenish able energy resources, the energy level is a monotonically decreasing function. The updated energy level should never be higher than the predicated energy level since the predicted energy level is calculated based on only the actually detected usage. If the updated energy level is higher than the predicted level, the node must have been compromised and should be excluded from its list of the adjacent neighbouring grids.

3.5 Energy efficiency and energy balance

The CASER is designed to balance the overall sensor network energy consumption in all grids by controlling energy spending from sensor nodes with low energy levels. In this way, extend the lifetime of the sensor networks. Through the EBC a, energy consumption from the sensor nodes with relatively lower energy levels can be regulated and controlled. Therefore, effectively prevent any major sections of the sensor domain from completely running out of energy and becoming unavailable.

In the CASER scheme, the parameter a can be adjusted to achieve the expected efficiency. As increases, better energy balance can be achieved. Meanwhile, the average number of routing hops may also increase. In other words, though the energy control can balance the network energy levels, it may increase the number of routing hops and the overall energy consumption slightly. This is especially true when the sensor nodes have very unbalanced energy levels. Balance the overall sensor network energy consumption in all grids. In this way, we can extend the lifetime of the sensor networks. By preventing attack, reduce the jamming with the help of CASER, network can achieve good energy efficient and balance the energy over the network**.**

3.6 CASER Advantage

- Balanced the energy consumption
- Increase the network lifetime
- Flexibility to support multiple routing strategies
- Excellent routing performance
- Provide the more secure for packet and also routing

4. Conclusions

Using probabilistic forwarding to send traffic on different routes provides an easy way to use multiple paths without adding much complexity or state at a node. A secure and efficient Cost- Aware SEcure Routing (CASER) protocol for WSNs to balance the energy consumption and increase network lifetime. CASER has the flexibility to support multiple routing strategies in message forwarding to extend the lifetime while increasing routing security. Both theoretical a results show that CASER has an excellent routing performance in terms of energy balance and routing path distribution for routing path security. We also proposed a non-uniform energy deployment scheme to maximize the sensor network lifetime. The proposed schemes can achieve very good performance in energy consumption, message delivery latency and message delivery ratio.

ACKNOWLEDGMENT

This research was supported by my Head of the Department, Prof.T.R.Srinivasan. We thank Mr.Chandra Mohan for assistance with a technique and Mr.Sathish for comments that greatly improved the manuscript. We thank famous persons Dr.Karunanithi and Dr.K.C.K.Vijayakumar, for sharing their pearls of wisdom with us during the course of this research, and we thank Mr.J.Jeyaram and Mr.R.Rajagopal reviewers for their so-called insights. We are also immensely grateful to family for their comments and support, although any errors are our own and should not tarnish the reputations of these esteemed persons.

References

[1] J.-H. Chang and L. Tassiulas, “Maximum lifetime routing in wire- less sensor networks,” IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 609–619, Aug. 2004.

[2] H. Zhang and H. Shen, “Balancing energy consumption to maxi- mize network lifetime in data-gathering sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 10, pp. 1526–1539, Oct. 2009

[3] C.-C. Hung, K.-J. Lin, C.-C. Hsu, C.-F. Chou, and C.-J. Tu, “On enhancing network-lifetime using opportunistic routing in wire- less sensor networks,” in Proc. 19th Int. Conf. Comput. Commun. Netw., Aug. 2010, pp. 1–6.

[4] C. Ozturk, Y. Zhang, and W. Trappe, “Source-location privacy in energy-constrained sensor network routing,” in Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw., 2004, pp. 88–93.

[5] Y. Li and J. Ren, “Preserving source-location privacy in wireless sensor networks,” in Proc. IEEE 6th Annu. Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw., Rome, Italy, Jun. 2009, pp. 493–501.

[6] M. Shao, Y. Yang, S. Zhu, and G. Cao, “Towards statistically strong source anonymity for sensor networks,” in Proc. IEEE 27th Conf. Comput. Commun., Apr. 2008, pp. 51–55.

[7] Y. Li and J. Ren, “Source-location privacy through dynamic rout- ing in wireless sensor networks,” in Proc. IEEE INFOCOM 2010, San Diego, CA, USA., Mar. 15–19, 2010. pp. 1–9.

[8] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source-location privacy in sensor network routing,” in Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2005, pp. 599–608.

[9] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor net- works: Attack and defense strategies,” IEEE Net., vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[10] A. Pathan, H.-W. Lee, and C. seon Hong, “Security in wireless sensor networks: Issues and challenges,” in Proc. 8th Int. Conf. Adv. Commun. Technol., 2006, pp. 1043–1048.

[11] Y. Li, J. Li, J. Ren, and J. Wu, “Providing hop-by-hop authentication and source privacy in wireless sensor networks,” in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

[12] B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., New York, NY, USA, 2000, pp. 243–254.

[13] Y. Yu, R. Govindan, and D. Estrin, “Geographical and energy- aware routing: A recursive data dissemination protocol for wireless sensor networks,” Comput. Sci. Dept., UCLA, TR-010023, Los Angeles, CA, USA, May 2001.

[14] R. Shah and J. Rabaey, “Energy aware routing for low energy ad hoc sensor networks,” in Proc. IEEE Wireless Commun. Netw. Conf., Mar. 17–21, 2002, vol. 1, pp. 350–355.