Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 169-174, 2016
ISSN 1990-9233;

DOI: 10.5829/idosi.mejsr.2016.24.TAET23423

Fake Content Delivery Using Replacement Algorithm In Wireless Sensor Networks

[1]R. Keerthana and [2]M.M. Kokila

[1]Department of Computer Science and Engineering (With Specialization in Networks,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India
[2]Department of Computer science and Engineering,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India

Abstract: Security and Lifetime optimization are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-replenishable energy resources. A novel secure and efficient Cost-Aware Secure Routing (CASER) protocol to deal with these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic-based random walking. In the network topology given, energy consumption is disproportional to uniform energy deployment which 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. The theoretical analysis results demonstrate that the proposed CASER protocol can provide an excellent tradeoff between routing efficiency and energy balance and can significantly extend the lifetime of the sensor networks in all scenarios. And also it delivery some meaningless file which is we declared inside virtual buffer to the hacker.

Key words: Routing · Security · Energy Balance · Energy Efficiency

INTRODUCTION

A wireless sensor network (WSN) (sometimes called a WSAN (Wireless Sensor and Actor Network)) are spatially distributed autonomous sensors to environmental conditions or monitor physical, such as pressure, temperature, sound, etc. and to cooperatively pass their data through the network to a core location. The more modern networks are bi-directional which enabled the control of sensor activity. WSN [1] development was motivated by military applications such as battlefield inspection; today such networks are used in many industrial and consumer applications, such as machine health, industrial control and process monitoring and so on. Many nodes built together to form "nodes" from a few to several hundreds or even thousands. In this each node is joined to one sensor.

Each such sensor network node has typically some parts: a radio transceiver with an interior 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 [2]. A bridge is provided between the real physical and virtual worlds which allows the ability to observe the up to that time unobservable at a fine resolution over large spatiotemporal scales. A wide range of application like potential applications to science, civil infrastructure, industry, transportation and security. Finally, we put forward some open issues regarding the design of hierarchical WSNs. This analysis aims to provide useful guidance for system designers on how to select and evaluate appropriate routing protocols and logical topologies for specific applications.

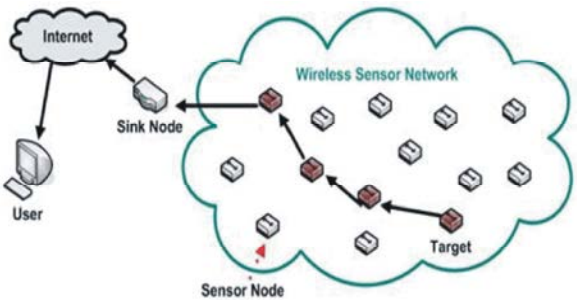


Fig. 1: Wireless sensor networks

Corresponding Author: R. Keerthana, Department of Computer Science and Engineering (with Specialization in Networks, Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India.

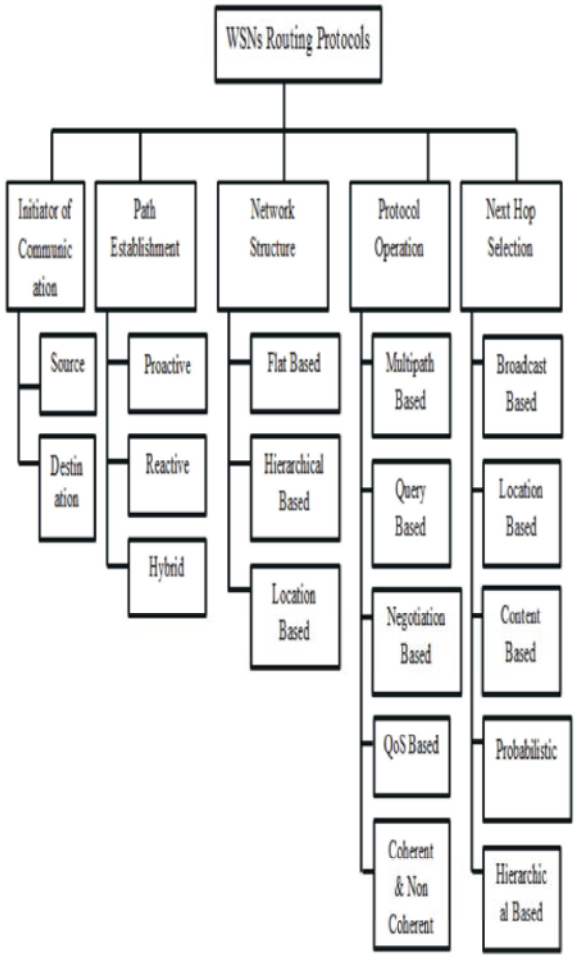


Fig. 2: Routing Protocol in WSNs

Routing Protocols In WSNs: Function of routing protocol is to specify how routers communicate with each other, disseminate information that enables them to select routes among any two nodes on a computer network. Routing algorithms find out the specific choice of route. Each router has a priori knowledge only of networks attach to it straight. A routing protocol shares this information first with immediate neighbors and then throughout the network. With this procedure, the topology information are grown in the network. Routing in wireless sensor networks differs from predictable routing in fixed networks in various ways. It is infrastructure less and these wireless links are unreliable. The sensor nodes may not succeed and routing protocols have to gather harsh energy saving requirements. Many routing algorithms were developed for wireless networks in common. Fig. 2 show the various routing protocols in WSNs.

The Adversarial Model: In WSNs, the adversary may try to improve the message source or jam the message from being delivered to the sink node. The adversaries aim at equip themselves with complex equipment's in a best way. Some technical advantages over the sensor nodes are:

- The adversaries consists of sufficient energy [3] resources, adequate computational capability and sufficient memory for data storage. On detecting an event, they could determine the immediate sender by analyzing the direction and strength of the signal they received. Without much of delay, this moves to the sender's location. They may also cooperation some sensor nodes in the network.
- The adversaries will not interfere with the right functioning of the network, such as altering the routing path, modifying messages, destroying sensor devices or modifying messages, since such activities can be simply known. The adversaries carried out passive attacks like eavesdrop on the communications.
- The adversaries monitors the traffic in any exact area that is important for them and find all of the transmitted messages in that area. In fact, if the adversaries could check the entire WSN, they can monitor the events directly without relying on other people's sensor network.

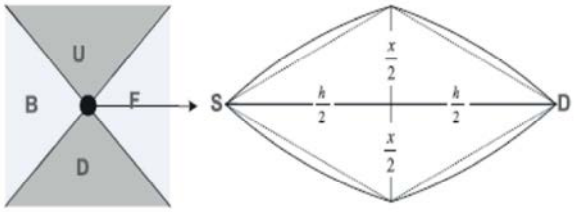
Security Goals In WSNs: A wireless sensor network shares some common features with the traditional network and also has unique features of its individual that distinguishes it from the traditional network. Security [4] goals or requirements covers both goals of traditional network and the goals suitable solely to the wireless sensor network.

Confidentiality is the means of restrictive information access to only the authorized users and preventing access or disclosure by the unofficial users. Data confidentiality is the most important issue that any network must address. If sensor nodes are not talented of keeping the data confidential, then any neighboring node can tamper with the data and transmit false information. This can cause serious hazards, particularly in military applications. *Data authentication* is the ability of a receiver to make sure that the data received by it is from a right sender. In a wireless sensor network, data can not only be tampered by the malevolent nodes but the entire

packet stream can be changed by addition of false packets to it. Data authentication can be achieved by symmetric key cryptography where the sender and receiver share a secret key or using asymmetric key cryptography where the data can be decrypted and encrypted using public and private keys. *Data Availability* is determined once the services of a network are available in the presence of attacks in it. A single point failure in the network can warn the availability of resources and other services. So, data availability is responsible for the operation and is of prime importance of the network. *Data Integrity* ensures that the received data is not altered in transfer. It confirms that the data is consistent and has not been altered or changed. The network must incorporate safety mechanisms against different attacks caused by malicious nodes so as to ensure integrity of the data.

Data Freshness determines that the data is new and no old packets have been replayed. It is essential to ensure the freshness of the message, apart from ensuring data integrity and confidentiality. Weak freshness that provides limited message ordering but doesn't give any delay information and strong freshness, which provides total delay estimation and message ordering. For sensor measurements, weak freshness is used while strong freshness is engaged in time synchronization in the network. *Self-Organization* sensor nodes in a wireless sensor network are randomly deployed and have no permanent 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 key management building trust relations and multi-hop routing, with the neighbors. If self-organizing capability lacks in a sensor network, then scratch resulting from attacks can be significant. *Time Synchronization* sensor network applications rely on some type 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 all sensor in the network. WSN is expected to locate faults needs accurate information about a position in order to indicate a fault's location. Unfortunately, a malicious node can manipulate non secured position information by reporting false signal strengths, replaying signals.

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 all grid with the highest energy level is selected as the head node or message forwarding. As well as, each node in the grid will maintain its own attributes, including location information remaining energy level of its grid, in addition to the attributes of its adjacent neighboring grids. The information maintained by each sensor node will be updated periodically. We assume that the sensor nodes in its direct neighboring grids are all within its straight communication range. We also presume that the whole network is fully connected through multi-hop communications [5, 6]. Additionally, the maintained energy levels of its adjacent neighboring grids are used to filter out and detect the compromised nodes for active routing selection.



(a) Next hop node distribution (b) Routing path

Fig. 3: Routing path and length

The shortest path routing also called deterministic routing, in this routing the next hop grid is selected from the neighbor 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 neighbor grid list for message forwarding. The routing path is more dynamic and unpredictable. So for an adversary, message capturing is more difficult. Therefore, the delivery ratio can be increased in a hostile environment. Using this routing we can avoid the jamming [7]. 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 neighbor node for all the node, select the neighbor node based on the communication range, 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 [8] 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 characterize by their target, to alter the path that the route takes through the system in response to a change in situation. The adaptation allows many routes as possible as to remain valid in reaction to the change. People using a transport system can display dynamic routing. For example of dynamic routing can be seen with in financial markets. For example, Adaptive Smart Order Router or ASOR, takes routing decisions dynamically and based on real-time market events. Another 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.

Cost Aware Secure Routing Protocol: In CASER routing protocol, each sensor node needs to keep up the energy levels of its immediate neighboring neighboring grids in addition to their relative locations. Using this information, every sensor node can create varying filters based on the needed design tradeoff between efficiency and security. The quantitative security analysis demonstrate the proposed algorithm can protect the source location information from the adversaries.

The main focus is on two routing strategies for message forwarding: secure message forwarding through random walking and shortest path message forwarding to create routing path unpredictability for source privacy [9, 10] and jamming prevention.

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 total number of messages that can be delivered and sensor network lifetime 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.

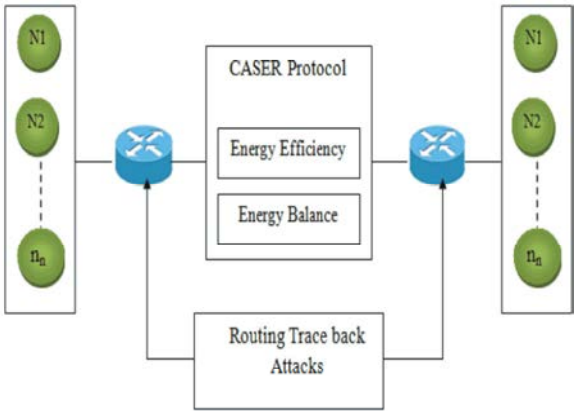


Fig. 3: CASER System Architecture

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 possible to be widely used in both civilian and military applications. A key feature of such networks is that each network consists of a large number of unattended and untethered sensor nodes. These nodes often have very limited and non-replenishable energy resources which make energy an main design issue for these network.

Secure Routing Protocol Design: Wireless sensor domain, anyone with an appropriate wireless receiver can monitor and intercept the sensor network communications.The CASER protocol planned 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 correctly designed routing protocol should not only ensure a high message delivery ratio and low energy consumption for message delivery, but also balance the full sensor network energy consumption and thereby extend the sensor network lifetime. 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, anyone with an correct wireless receiver can monitor and intercept the sensor network communications.

Routing Traceback Attacks: The routing [11] 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 upper than the predicated energy level since the level is calculated based on only the actually detected usage. If the updated energy level is higher than the predict level, the node must have been compromised and should be excluded from its list of the adjacent neighboring grids [12].

Energy Efficiency and Energy Balance: The CASER is designed to balance the overall sensor network energy consumption in all grids by calculating 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 totally running out of energy and becoming engaged.

In the CASER scheme, the parameter a can be adjusted to achieve the expected efficiency. And also increases, better energy balance can be achieve. 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 utilization 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 congestion with the help of CASER, network can achieve good energy efficient and balance the energy over the network.

Fake Content Delivery: By using this we can get high energy efficiency and balance the energy but the hackers again do some attack. To avoid it we also deliver the fake content for hackers. These will goings to show a virtual buffer content for normal view to keep another buffer for transmit file to receiver. In this method hacker get some meaningless file which is already declared inside virtual buffer. The process can be explained in Fig. 4.

Algorithm : Fake content replacement algorithm.
Input: Integer r, the number of replacement file
Input: Integer n, the number of nodes
Output: Replacement file

```
for all i such that 0 = i < n do
Preload node i's replace with i
end for
Circular-shift each column (j index) of Replacement by column index - 1
for all i such that 0 = i < n do
for all j such that 0 = j < r do
repeat
z = random content file
v = Replacement[z][j]
if v = i and Replace[i][j] = z then
valid replace = 1
    if valid replace then
    Replace[z][j] = Replace[i][j]
    Replace[i][j] = v
    end if
    end if
    end for
    end for
```

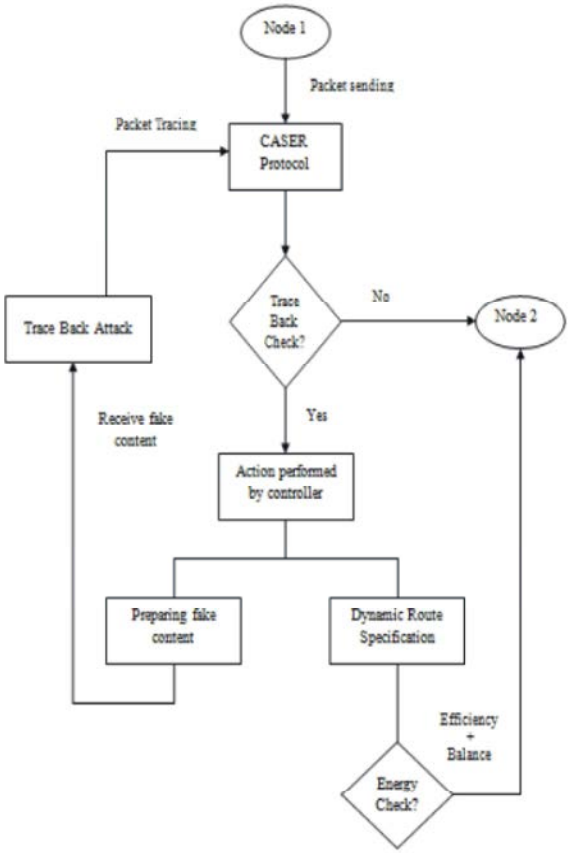


Fig. 4: Dataflow diagram

CASER Advantage:

- Balanced the energy utilization
- raise the network lifetime
- Flexibility
- Support multiple routing strategies
- Provide the more secure for packet and also routing
- Increased network reliability

CONCLUSIONS

Using probabilistic forwarding to send traffic on different routes provide a simple way to use various paths without adding much complexity or state at a node. An efficient and secure Cost- Aware SEcure Routing (CASER) protocol for WSNs to increase network lifetime and balance the energy consumption. CASER has the flexibility to carry several routing strategies in message forwarding to extend the lifetime while increasing routing safety. CASER has an excellent routing performance regarding routing path distribution and energy balance for routing path security. The 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 delivery the fake content to the traceback attacker so the file may more secure.

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 document. 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 reviewer for their so-called insights. We are also immensely grateful to family for their comments and support, even though any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

1. Chang, J.H. and L. Tassiulas, 2004. Maximum lifetime routing in wire- less sensor networks, IEEE/ACM Trans. Netw., 12(4): 609-619.
2. Zhang, H. and H. Shen, 2009. Balancing energy consumption to maximize network lifetime in data-gathering sensor networks, IEEE Trans. Parallel Distrib. Syst., 20(10): 1526-1539.
3. Ozturk, C., Y. Zhang and W. Trappe, 2004. "Source-location privacy in energy-constrained sensor network routing, in Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw., pp: 88-93.
4. Pathan, A., H.W. Lee and C. seon Hong, 2006. Security in wireless sensor networks: Issues and challenges, in Proc. 8th Int. Conf. Adv. Commun. Technol., pp: 1043-1048.
5. Li, Y., J. Li, J. Ren and J. Wu, 2012. Providing hop-by-hop authentication and source privacy in wireless sensor networks, in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, pp: 3071-3075.
6. Kamat, P., Y. Zhang, W. Trappe and C. Ozturk, 2005. Enhancing source-location privacy in sensor network routing, in Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst., pp: 599-608.
7. Xu, W., K. Ma, W. Trappe and Y. Zhang, 2006. Jamming sensor net- works: Attack and defense strategies, IEEE Netw., 20(3): 41-47.
8. Hung, C.C., K.J. Lin, C.C. Hsu, C.F. Chou and C.J. Tu, 2010. On enhancing network-lifetime using opportunistic routing in wire- less sensor networks, in Proc. 19th Int. Conf. Comput. Commun. Netw., pp: 1-6.
9. Li, Y. and J. Ren, 2009. Preserving source-location privacy in wireless sensor networks, in Proc. IEEE 6th Annu. Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw., Rome, Italy, pp: 493-501.
10. Li, Y. and J. Ren, 2010. Source-location privacy through dynamic routing in wireless sensor networks, in Proc. IEEE INFOCOM 2010, San Diego, CA, USA., 15-19, 2010. pp: 1-9.
11. Shao, M., Y. Yang, S. Zhu and G. Cao, 2008. Towards statistically strong source anonymity for sensor networks, in Proc. IEEE 27th Conf. Comput. Commun., pp: 51-55.
12. Karp, B. and H.T. Kung, 2000. GPSR: Greedy perimeter stateless routing for wireless networks, in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., New York, NY, USA, pp: 243-254.