I J C T A, 9(26) 2016, pp. 357-362

A Secure Energy Efficient and Aware Protocol for WSN

P. Thangaraju[1] and Kanjana S[2]

ABSTRACT

In any Wireless Sensor Network the basic problem of the Nodes is the energy levels and the lack of infrastructure for routing. Either the nodes become dead quickly due to lack of energy or the attackers destroy or compromise a node stealing data or jamming the nodes. Most existing solutions occupy more overheads than the data transmission itself and also have false positives or false negatives. They are not aware of the energy consumed by the nodes. The proposed solution aims to develop an efficient protocol which is energy aware of the nodes and also overcomes malicious jamming attacks apart from extending the lifetime of the node. The protocol is name as Hybrid CASER which also consumes less overheads, communication and bandwidth compared to the existing models.

Keywords: WSN, Energy Aware, Routing, Jamming Attacks.

1. INTRODUCTION

WSN's are increasingly being deployed for civilian, military and other applications because of their low cost and easy deployability. But some of the problems like energy efficiency, routing and malicious jamming attacks and routing traceback attacks are a cause of concern. Mainly energy cannot be replenished in most of the cases cause the network to be redundant soon. In energy aware routing the sink node distributes requests with geographic attributes to the destination region instead of using the usual flooding mode.

Next each node forwards messages to its neighboring nodes based on estimated energy cost where also the origin and location privacy are maintained. This is done through broadcasting model which combines valid messages with fake or dummy messages, which consumes significant amount of a node's energy. This also leads to network collisions and decreases the packet delivery ratio throughput.

Other models like the phantom routing protocol each message is routed from the actual sink to a phantom source along a predefined path. The direction of the path with nodes is stored in the message header while forwarding. The phantom node can be away from the actual origin node and unfortunately the message may sometimes be captured on the random walk path. Thus the adversaries are able to get the direction information from the message header. The other major drawbacks are higher energy consumption, increased network collision, reduced packet delivery ratio and attacks with not being able to provide full security for packets.

2. RELATED WORKS

Chalermek Intanagonwiwat *et. al.* [1] in their work in 2000 mentioned "Directed diffusion": a scalable and robust communication paradigm for sensor networks" mentioned Directed Diffusion which is a query based multi-path routing protocol, in which the sink initializes the routing process. Kamalrulnizam Abu Bakar

[1] Associate Professor, Department of Computer Applications, Bishop Heber College, Tiruchirappalli, India. *E-mail: thangarajubhc@yahoo.co.in*

[2] Research Scholar, Department of Computer Science, Bishop Heber College, Tiruchirappalli, India. *E-mail: kanjsm66@gmail.com*

MarjanRadi [2] *et. al.* in "Multipath routing in wireless sensor networks: Survey and research challenges" in 2012 mentioned tolerant routing. Here an interest message received by the nodes creates a gradient to the node from which the message is received. Ganesan Deepak [3] *et. al.* in "Highly-resilient energy-efficient multipath routing in wireless sensor networks" mentioned Braided Multipath Routing Protocol which provided fault tolerant routing in WSN through constructing several partially disjoint paths similar to Directed Diffusion.

Ye Ming Lu and Vincent W. S. Wong [4] in their work "An energy-efficient multipath routing protocol for Wireless Sensor Networks" in 2007 proposed a distributed, scalable and localized multi-path search protocol, used to discover multiple paths between the sink and source nodes in a disjointed manner and implemented a load balancing algorithm to distribute the data packets over the discovered multiple paths along differing routes. Philipp Hurni and Torsten Braun [5] mentioned Energy-efficient multi-path routing in wireless sensor called AOMDV-Inspired Multi-path Routing Protocol which is designed based on the AOMDV (multi-path version of AODV, to attain energy efficient and low-latency communication in wireless sensor networks by using cross layer information. Jenn-YueTeo [6] *et. al.* in their paper "Interference minimized multipath routing with congestion control in wireless sensor network for high-rate streaming" in 2008 Interference-Minimized Multipath Routing Protocol (I2MR) aimed to support high data rate streaming in wireless sensor networks

W. Heizelman [7] *et. al.* in their work "Energy-efficient communication protocol for wireless micro sensor networks author mentioned novel clustering based routing protocol LEACH acronym for Low-Energy Adaptive Clustering Hierarchy". This model reduced global energy usage by sharing the load and energy among all the sensor nodes at different points in time in the given wireless sensor network. J. M. Kim *et. al.* [8] in their work "CHEF: Cluster head election mechanism using fuzzy logic in wireless sensor networks" presented a novel approach for cluster head election in wireless sensor network. The mentioned approach is more appropriate for electing cluster-heads for medium sized clusters. The cluster heads closer to the base station are loaded with heavy traffic and tend to die early. C. Li *et. al.* [9] in "An energy efficient unequal clustering mechanism for wireless sensor networks" in 2005mentionedthe new an Energy Efficient Unequal Clustering (EEUC) mechanism in wireless sensor networks to solve this issue. M. Handy *et. al.* [10] in "Low energy adaptive clustering hierarchy with deterministic cluster-head selection" in 2002 extended the existing protocol LEACH-Low-Energy Adaptive Clustering Hierarchy which reduces the power utilization of wireless micro sensor networks. Based on network configuration a network lifetime of micro sensor networks is increased by 30 percent.

Geographic routing protocols utilize the geographic location information to route data packets hop-to-hop from the source to the destinaion[12]. The basic idea is to set the local topology of the network as planar graph and then the relay nodes try to forward messages along one or possibly a sequence of adjacent faces toward the destination. Lifetime is another area that has been extensively studied in WSNs [13]. Then [14] investigated the unbalanced energy consumption for uniformly deployed data-gathering sensor networks. In this paper, the network is divided into multiple corona zones and each node can perform data aggregation. A localized zone-based routing scheme was proposed to balance energy consumption among nodes within each corona.

The authors in [15] formulated the integrated design of route selection, traffic load allocation and sleep scheduling to maximize the network lifetime. Based on the concept of opportunistic routing, [16] developed a routing metric to address both link reliability and node residual energy. The sensor node computes the optimal metric value in a localized area to achieve both reliability and lifetime maximization.

In addition, exposure of routing information presents significant security threats to sensor networks. By acquisition of the location and routing information, the adversaries may be able to trace back the source node easily. To solve this problem, several schemes have been proposed to provide source-location privacy

through secure routing protocol design [17] and [18]. In [19], source-location privacy is provided through broad-casting that mixes valid messages with dummy messages. The main idea is that each node needs to transmit messages consistently. Whenever there is no valid message to transmit, the node transmits dummy messages. The transmission of dummy messages not only consumes significant amount of sensor energy, but also increases the network collisions and decreases the packet delivery ratio. In [20], [21], the messages is first transmitted to a randomly selected intermediate node in the sensor domain before the messages is being forwarded to a network mixing ring where the messages from different directions are mixed. Then the message is forwarded from the ring to the sink node.

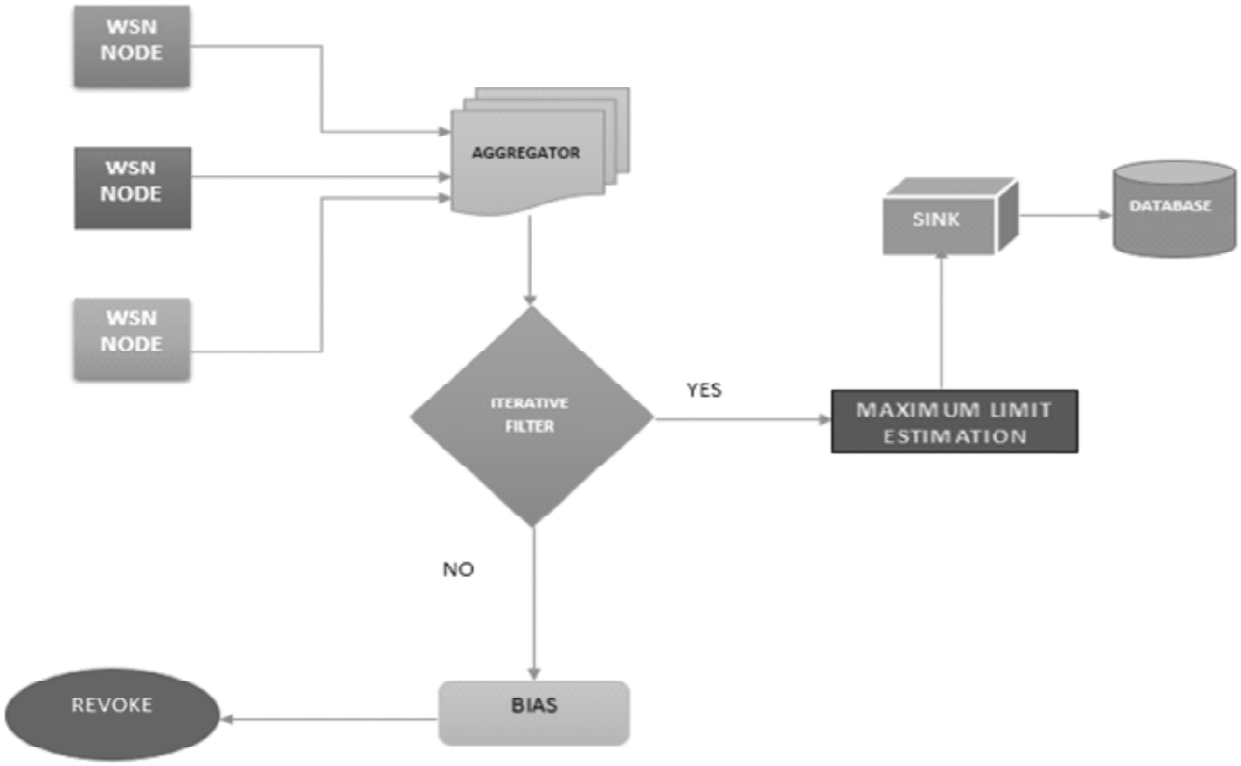
3. PROPOSED ARCHITECTURE

The WSN are placed in a remote locations with a sink connected to the network. According to the number of cluster heads, the nodes are randomly placed in a network. As events occur randomly the WSN'S transmit the data's to the sink node or master node. Each node is assumed to be calculating the energy independently.

The data transmissions between nodes are and their paths are calculated by the number of packets transmitted. The Virtual Coordinates improved the direction using the CAESAR protocol All the information are thus split up and then transmitted after encryption using the algorithm and transmitted securely. Any particular node's locations and its subsequent topologies are based on the relative movement of packets to the appropriate location in the multi-hop path using the HCAESAR protocol.

The mentioned topology CAESAR method shows that the method provides both higher accuracy and better security to collusion attacks when compared with the existing methods. To the best of knowledge, no existing work addresses on false data injection for a number of scenarios. The proposed model addresses all the drawbacks of the existing models in terms of time delay and hops during routing.

The advantages may be summarized as follows. HCAESARs overcome many of the demerits of VCS when match up with the geographical coordinate systems. But without inheriting its disadvantages, while preserving all the advantages of connectivity-based VCs HCAESARS have the ability to do visualization



without the need for analog measurement capability. That too at nodes will be invaluable for networks whose nodes are extremely limited in capability (energy, security and memory). Topology coordinates provide an economical alternative to physical coordinates for many sensor networking algorithms.

3.1 ALGORITHM–HCAESAR (Hybrid Cost-Aware Secure Routing)

Step 1: A node encounters for the first time,

Step 2: It randomly generates a path with the neighbour node computes, sends to, and stores a code.

Step 3: Now other resultant paths are checked for the coordinates to move the packets

Step 4: The topology and the number of packets to be transmitted by each of the packets are calculated by HCAESAR

Step 5: Next the packets are encrypted using 3DES

Step 6: The split packets are randomly interspersed

Step 7: These packets are transmitted via the virtual nodes.

Step 8: Finally the packets reach the sink via different routes.

Step 9: Decryption is done and original message is retrieved.

3.2 COMPUTATION

Divide the whole sensor domain into four equal size sections *F*, *B*, *U* and *D*. Let P_F, P_B, P_U and P_D be the probabilities that the message is forwarded to the sections F, B, U and D respectively. Then we have the following theorem.

$$\frac{h\sqrt{1+\left(\frac{P_U+P_L}{P_F-P_B}\right)^2}}{P_F-P_B}$$

4. EVALUATIONS AND DISCUSSIONS

Thus from the above tables it is clear that the routing hops for the HCAESAR model is less than the existing models and also the time delay for security that is encryption is also considerably less when compared with the earlier models.

Table 1
Parameters comparison in existing and proposed methodologies

Routing Hops	*Existing*	*HCAESAR*
1	10.5	8
2	11.02	9.3
3	11.15	10.5

Table 2: Parameters comparison in existing and proposed methodologies

Security	*Existing*	*HCAESAR*
Time delay	0.0344	0.0155

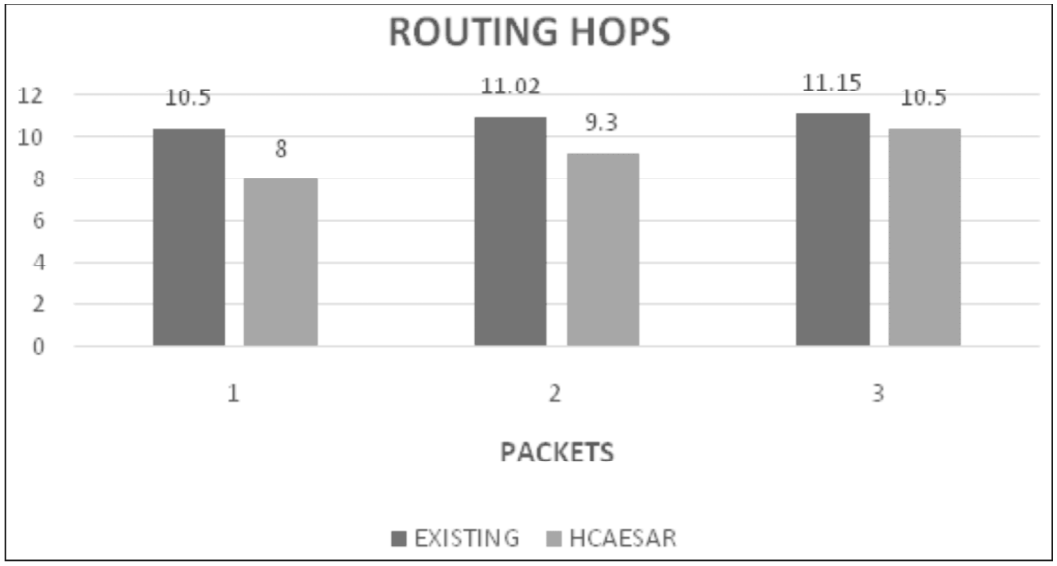


Figure 1: Representation of existing and proposed methodologies (Routing Hops)

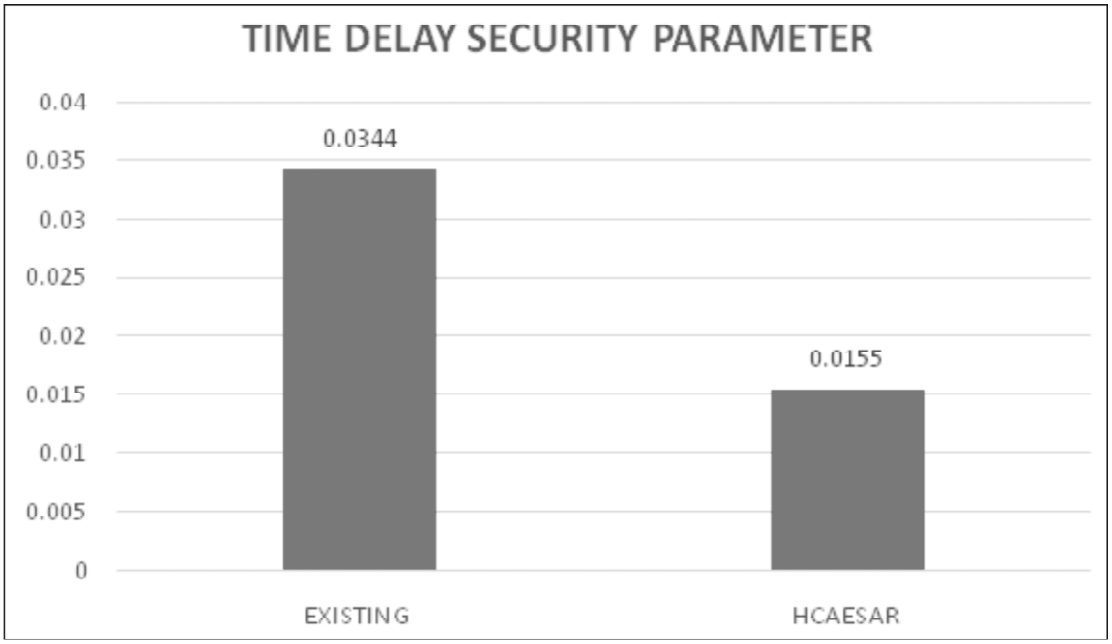


Figure 2: Representation of existing and proposed methodologies (Time Delay Security Parameter)

CONCLUSION

The proposed model is a secure and energy aware Hybrid Cost Aware Secure Routing (HCASER) protocol that can address both energy balance and safe routing dynamically in WSNs. The HCASER routing protocol maintains the energy levels of its neighboring grids containing nodes in addition to their relative positions, secondly this information is used for forwarding to each sensor node. The final quantitative security analysis demonstrates the proposed algorithm not only protects the origin node and its location but also the information from the adversaries in case of jamming and traces back attacks. The focus is to develop two routing strategies for message forwarding apart from finding the shortest path message for forwarding the event data by forwarding through random walking path to confuse and create unpredictability for source privacy and jamming attack prevention. The advantages of proposed system are reduced the energy consumption, secure packet forwarding and routing increased message delivery ratio and reduced the time delay. Thus the proposed HCASER model is effective in energy consumption apart from providing increased throughput in

delivering message packets. Also it counters attacks like trace backs and jamming. The lifetime of the network is extended well and shows considerable energy savings with low communication overheads. The model is self-adaptive and can be ported to other mobile wireless networks in the future.

REFERENCES

[1] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin. "Directed diffusion: a scalable and robust communication paradigm for sensor networks". *International conference on Mobile computing and networking*, 56–67, New York, 2000.

[2] Kamalrulnizam Abu Bakar Marjan Radi, Behnam Dezfouli, Malrey Lee," Multipath routing in wireless sensor networks: *Survey and research challenges. MDPI Sensors*, 650–685, January 2012.

[3] Ganesan Deepak, Govindan Ramesh, Shenker Scott, Deborah Estrin, "Highly-resilient energy-efficient multipath routing in wireless sensor networks", *ACM International symposium on Mobile ad hoc networking & computing*, MobiHoc'01, 251–254, New York, NY, USA, 2001.

[4] Ye Ming Lu, Vincent W. S. Wong," An energy-efficient multipath routing protocol for wireless sensor networks", *International Journal of Communication Systems*, vol. **20(7)**, 747–766, July 2007.

[5] Philipp Hurni and Torsten Braun. Energy-efficient multi-path routing in wireless sensor networks", *7th international conference on Ad-hoc, Mobile and Wireless Networks*, Berlin, Heidelberg, Springer-Verlang,72–85, 2008.

[6] Jenn-Yue Teo, Yajun Ha, Chen-Khong Tham," Interference-minimized multipath routing with congestion control in wireless sensor network for high-rate streaming", *Mobile Computing, IEEE Transactions* on, vol. **7(9)**, 1124–1137, 2008.

[7] W. Heizelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficient communication protocol for wireless micro sensor networks," *International Conference on System Sciences(HICSS),* Maui, HI, 3005-3014, 2000.

[8] J. M. Kim, S. H. Park, Y. J. Han, and T. M. Chung, "CHEF: Cluster head election mechanism using fuzzy logic in wireless sensor networks, "*International Conference on Advanced Communication Technology (ICACT)*, 654-659, 2008.

[9] M. Handy, M. Haase, D. Timmermann, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection," in the 4th *International Workshop on Mobile and Wireless Communication Network*, Citeseer, 368-372, 2002.

[10] C. Li, M. Ye, G. Chen, and J. Wu, "An energy efficient unequal clustering mechanism for wireless sensor networks," in *IEEE International Conference on Mobile Ad hoc and Sensor Systems Conference (MAHSS)*, 597-604, 2005.

[11] F.Bouhafs, M. Merabti, and H. Mokhtar, "A Semantic Clustering Routing Protocol for Wireless Sensor Networks", *IEEE Communications Society subject matter experts for publication in the IEEE CCNC2006* proceedings, 2006.

[12] Y. Li, J. Li, J. Ren, and J. Wu, "Providing hop-by-hop authentication and source privacy in wireless sensor networks", *in IEEE INFOCOM 2012 Mini-conference,* Orlando, Florida, USA, March 25-30,2012.

[13] Y. Li, Y. Yang, and X. Lu, "Rules of designing routing metrics for greedy, face, and combined greedy-face routing", *Mobile Computing, IEEE Transactions* on, vol. 9, no. **4**, 582-595, April 2010.

[14] H. Zhang and H. Shen, "Balancing energy consumption to maximize network lifetime in data-gathering sensor networks", Parallel and Distributed Systems, *IEEE Transaction on*, vol. 20, no. **10**, 1526-1539, Oct 2009.

[16] F. Liu, C.Y. Tsui, and Y.J. Zhang, "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks", *Wireless communications, IEEE Transactions* on, vol. 9, no **7**, 2258-2267.

[17] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks", in Proceedings of *IEEE SECON* 2009, Rome, Italy, June 22-26, 2009.

[18] San Diego, "Source location privacy through dynamic routing in wireless sensor networks", in Proceedings of *IEEE INFOCOM 2010*, USA, March 15-19, 2010.

[19] M. Shao, Y. Yang, S. Zhu and G. Cao, "Towards statistically strong source anonymity for sensor networks", in INFOCOM 2008. The *27th conference IEEE on Computer Communications*, 51-55, April 2008.

[20] W. Xu, K. Ma, W. Trappe and Y. Zhang, "Jamming sensor networks: attack and defense strategies", *IEEE Networks*, vol. 20, no. **3**, 41-47, 2006.

[21] A. Pathan, H. W. Lee and C. Seon Hong, "Security in wireless sensor networks: issues and challenges", in *The 8th International conference on Advanced communication Technology (ICACT),* vol. **2**, 48-55, 2006.

[22] P. Thanagaraju and S. Kanjana, "Survey About A Secure Energy Efficient Protocol for WSN" *International Journal of Applied Engineering Research (IJAER),* 2016.