SYSTEMATIC CLUSTER HEAD AND OPTIMIZED AUTHENTICATION BASED ROUTING IN WIRELESS SENSOR NETWORKS

B. Nancharaiah, Professor and Head of the Department
B. Vamsi Priya, G. Bhargavi, A. Narasimha Raju
Department of Electronics and Communication Engineering,
Usha Rama College of Engineering and Technology, Telaprolu, 521109.

Abstract:

Wireless sensor network (WSN) comprises of multiple nodes which are utilized in data transfer by forming short links between them. This results in large energy consumption so there is necessity of an efficient protocol. In this work a grid based communication network is established by formation of clusters and selecting heads among the cluster , routing path and providing authentication to enhance privacy of data .The proposed technique improves when compared with existing technique the parameters like packet delivery ratio, energy consumption, end-to-end delay and throughput.

Index terms: Wireless Sensor Network, Cluster Head, Optimization, Hash Authentication, Deployment.

1. Introduction:

In fast-growing technological world, there is a vital role that data plays. To fulfil the requirements of the present generation, like speed of the data transfer, security, low power consumption etc, then there araised the wireless sensor networks. Wireless sensor networks (WSN) is a distributed network comprises of numerous nodes deployed in various geographical location. These nodes are dedicated to a particular task and employed to serve the operations like sensing the information in the particular region, store and process the information

The WSN senses multiple wireless standards like IEEE 801.11 and IEEE 801.15 variances in addition to GPS as needed mostly uses star topology, the mobility depends on the needs of the application and environment deployed in, as WSN nodes are self-driven. The main theme of our work is deployment of wireless sensor network is to decrease the energy utilization in the communication system through clustering. In the process of clustering, one node is chosen to be a group head of the cluster. The cluster head (CH) handles large part of the data processing steps in sensor nodes and cluster computation.

The most imperative limitations of existing techniques in WSNs are to control the rate of energy consumption and providing security to the system. This ought to be incorporated by effective routing techniques and communication strategy. The routing algorithm we used in our work is AODV (Ad hoc on demand distance vector) a reactive routing protocol which overcomes the drawbacks of dynamic source routing (DSR) like fast delivery of data packets accurately, and can handle multiple routes. So as the AODV routing protocol is considered as energy efficient we use this protocol in our proposed ASRC (authentication based secure routing clustering) approach as shown in fig.1 which provides secured authentication to access privacy of data and prevent data loss during transfer.

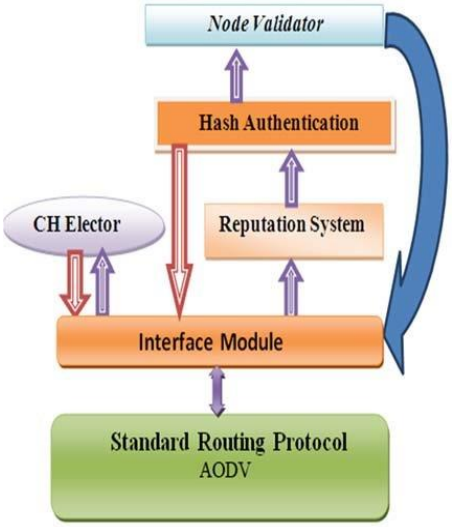

Fig.1: Block Diagram of ASRC-WSN

2. Existing Techniques:

There are many techniques proposed to attain energy efficient routing mechanism but there a raised the security threats when the node is assumed to be carrying continuous data transmission, that is replication process is being done.

The various routing techniques like PSO (particle swarm optimization), fuzzy based theory, DSR (dynamic source routing), LEACH (low energy adaptive clustering hierarchy), flower pollination technique. But all these techniques and multiple approaches to reach our final goal does not satisfied, many characteristics like the process of finding the shortest path, the node can select any analogous node in the network irrelevant of whether it belongs to the same network of different group and this process is found to be a major issue during the data transmission. Thus Ad hoc On Demand Distance Vector (AODV) mechanism has been developed along with the adoption of distributed clustering algorithm for cluster head selection. An experimental analysis is carried out through network simulators along with effective parameters such as packet delivery ratio (PDR), end to end delay and throughput.

3. Proposed Approach:

In this proposed work the goal is to identify, discover and maintain the optimal route between source and destination node in order to send/receive data packets and informative. Ad-Hoc On-Demand Distance Vector Routing (AODV), the source node and destination nodes IP addresses are already known. The protocol comprises of two counters (which includes SEQ no, ID of source and destination nodes),each node comprises of a routing table and along with these Route Request(RREQ) and Route Response(RRESP) packets are used in which RREQ is responsible for discovering of route from source to destination and RRESP sends back the route information response to its source. RREQ {Destination IP, Destination Sequence Number, Source IP, Source Sequence Number, Hop Count}.

Considering the main theme our research methodology the process of ours is mainly rotates around the basic three steps that are handled between source and destination nodes.

The basic operations involved are:

- Cluster head selection
- Optimized routing path
- Providing secured authentication

Wireless sensor networks are spatially dispersed nodes in a particular geographical location, so the numerous nodes irrespective of the number, type, size, capacity opted for the purpose of data transmission. Let us know in detail about the prior operations involved.

3.1Cluster Head Selection:

A group of nodes located in a region are to be considered as a cluster and this process is known as cluster formation, it is not mandatory to have equal number of nodes in each cluster. Depending on the amount of energy needed to be transferred the clusters are formed. Selecting the head of the cluster is a four step mechanism.

I. *Status Updater*: This lower level module will run inside every sensor's firmware to update all sensor related parameters to other peer sensors over the network. The critical sensor status such as packet transmission statistics, energy status, location, transmission power will be exchanged over the wireless link.

II. *Reputation Manage*r: This module takes input from the status updater and manages the reputation information of all the nearby neighbours of a sensor node.

III. *CH Decision:* This module performs the key operation of electing a Cluster Head within a cluster by consulting the feedback from the earlier reputation manager module. In this process, a peer who will be found to have highest reputation and energy and also located about the centre position of the cluster will considered to be the most acceptable candidate for CH entity. The centre location for CH is preferred because of uniform coverage and maximum reachability throughout the cluster, which ensure
enhanced coordination and communication between CH node and other sensors.

IV. *CH Declaration*: Once the CH entity inside each cluster is determined, every participating sensor node broadcasts this information throughout the cluster in the form of a declaration message. The message received by other cluster members including CH node within that cluster analyses this declaration message by comparing the self-node id with the declared CH ID to check if it's the newly elected CH. Whenever the selected CH node receives multiple such declaration messages from other cluster member, it is found that the declared node id to be equal with self id. It then declares itself as the CH in that cluster and acknowledges its new identity by replying the original declaration message.

The figure.2 and figure.3 displays the cluster formation and cluster head selection.

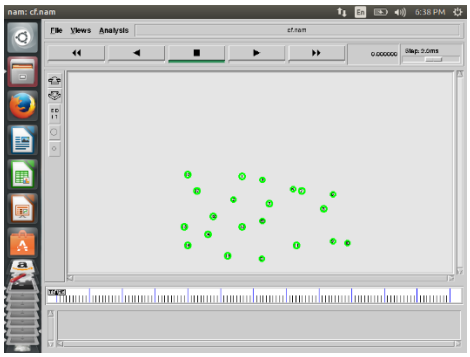

Fig.2: Cluster Formation

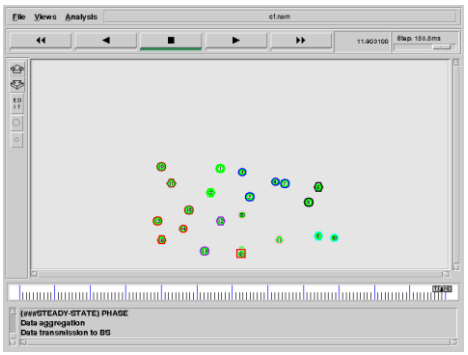

Fig.3: Cluster Head Selection

3.2. OPTIMIZED ROUTING:

The routing can be explained by the working principle of AODV routing protocol. When a node wishes to send a packet to destination, it checks the routing table to determine the current route, if YES it initiates the path formation elsewhere discovers a route process.

I. Route discovery path begins with Route Request (RREQ) packet source node creates it.

II. It contains – source node's IP address, SEQ number, destination IP address, SEQ number, broadcast ID number.

III. Broadcast ID gets incremented each time a source node uses RREQ.

As in WSN the nodes are self-configurable the source and destination are pre-determined. So, they provide an acknowledgement whether the path is found or not that is RREP (route reply) packet to the source. Thus, the routing path process till it finds the optimized path in the given cluster.Fig.4 shows the ASRC core state meachine

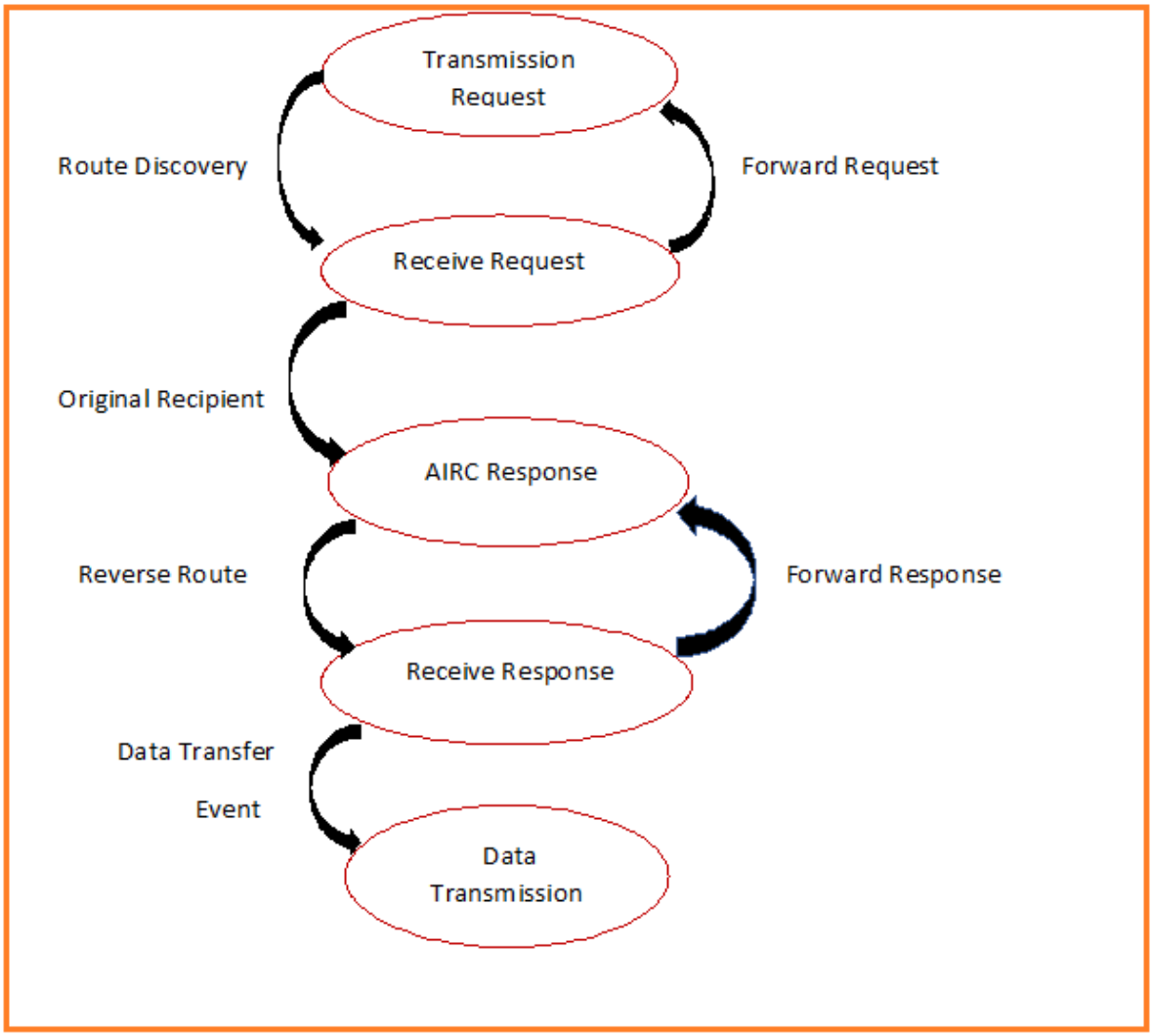

Fig.4: ASRC core state machine

3.3. Providing Secured Authentication:

The privacy threatens impacts a lot in the cut throat competition of the ruling technology so there is a need to apply certain measures to prevent the data from hackers, third party users. So, there is a key provided that is accessible by the destination node itself only the keys possessed by a standard node consists of a cell key, master key, EBS keys, and paired keys. The CH will only broadcast m rekeying messages for notifying all further nodes for updating by the properties of EBS scheme. Update messages must of course consist of the recalled node ID and all replacing keys, apart from being encrypted using elliptic curve. Rekeying procedure for compromised CH as the CH present in every cell act as a KDC, when a CH gets compromised, not only the particular keys such as cell key, master key, and paired key owned privately.

4.SIMULATION RESULTS: The simulation environment work is tabulated in table.1

SIMULATION TABLE.1:

Parameter	**Value**
Channel type	Wireless channel
MAC type	MAC 802_11g
Network interface type	Wireless
Routing type	AODV
Network size	1000*1000 sq. m
Antenna model	Omni directional antenna
Transmission type	UDP
Bit rate type	CBR
Number of nodes	21

The comparisons between existing and proposed approach is displayed in table.2.

PERFORMANCE TABLE.2: Simulation results at 10ms.

Parameter	HHSRP	ASRC
Throughput	681.44kbps	745.7kbps
End to End delay	2.19ms	1.81ms
Packet Delivery Ratio	89.00%	93.50%
Energy Consumption	2.06 J	0.816 J

The results are displayed for Packet Delivery Ratio (PDR), Throughput, Energy consumption and Delay in fig.5, fig.6, fig.7 and fig.8 respectively.

SIMULATIONS:

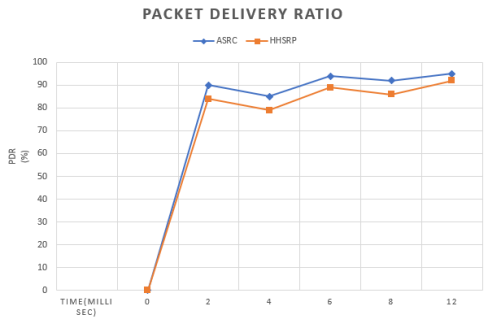

Fig.5:Packet Delivery ratio

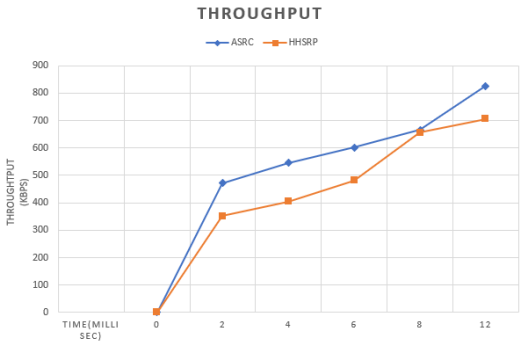

Fig.6: Throughput

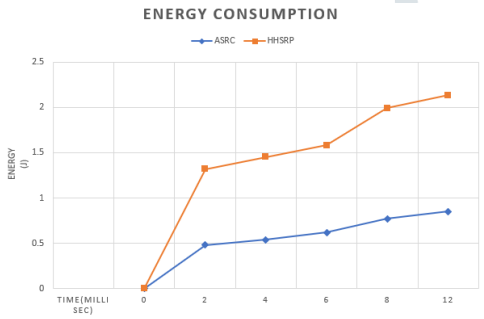

fig.7:Energy consumption

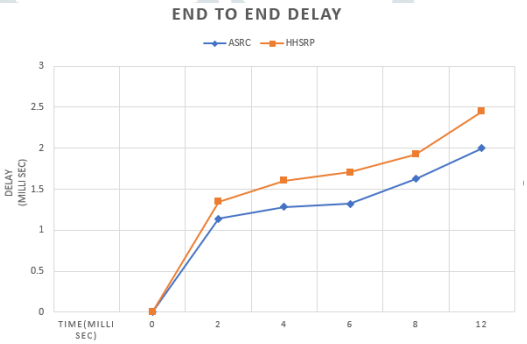

Fig.8: End to End Delay

CONCLUSION:

The proposed paper has compared the performance of HHSRP (hybrid hierarchical secured routing protocol) approach and ASRC (authentication based secure clustering) approach that are implemented on the basis of AODV routing protocol. The proposed approach is applied with DES-SHA (data encryption system-secured hash authentication). So, the energy consumed is minimized compared to the existing approach and hash-based authentication deals with the threats of privacy.

References

[1] Dargie, W. and Poellabauer, C. (2010). Fundamentals of wireless sensor networks: theory and practice. John Wiley and Sons. pp. 168–183, 191–192.

[2] Waleed Kh. Alzubaidi, Shaimaa H. Shake Efficient Cluster Head Selection and Optimized Routing in Wireless Sensor Network" Journal of Theoretical and Applied Information Technology28th February 2019. Vol.97. No 4

[3] Rao, P. S., Jana, P. K., & Banka, H. (2017). A particle swarm optimization-based energy efficient cluster head selection algorithm for wireless sensor networks. Wireless networks, 23(7), 2005-2020.

[4] Rama Krishnan, S., & Shyry, S. P. (2017, February). Fuzzy-based cluster head election mechanisms for wireless sensor networks: A review. In Information Communication and Embedded Systems (ICICES), 2017 International Conference on (pp. 1-6).

[5] Kaur, J., Randhawa, S., & Jain, S. (2018). A novel Energy Efficient Cluster Head Selection Method for Wireless Sensor Networks.

[6] Chen, T. S., Wang, N. C., & Wu, J. S. (2016). An efficient adjustable grid-based data replication scheme for wireless sensor networks. Ad Hoc Networks, 36, 203-213.

[7] Gielow, F., Jakllari, G., Nogueira, M., & Santos, A. (2015). Data similarity aware dynamic node clustering in wireless sensor networks. Ad Hoc Networks, 24, 29-45.