Power Efficient Broadcast Authentication and Routing Protocol for Wireless Sensor Networks

Nikita Kaushik
Swati

***Abstract*—Wireless Sensor networks incorporate of limited battery powered sensor nodes are set out to collect effective data from the field. To collect this information besides energy security is also a big issue. Source authentication is one of the desired security requirements. Thus, acquiring sensed information in both secure and energy efficient way is crucial to operate sensor networks for a long period of time. This paper presents a power efficient broadcast authentication and routing protocol for wireless sensor networks, called PEBARP that provides source authentication with minimum energy consumption using hierarchical clustering to partition the network into static clusters. It uses momentary cluster-heads to allocate the energy amount along with by immense power sensor nodes, thus enlarge network life-span. We performed here simulation-based assessment to examine the effectiveness of this proposed protocol across BMU (broadcast-multicast-unicast) routing algorithm. Experimental outcome confirms that PEBARP surpass BMU in terms of energy consumption minimization.**

Keywords—Wireless Sensor Networks(WSN); Hierarchical Clustering; Broadcast Authentication; Network Lifetime; Intermediate nodes(IN).

I. INTRODUCTION

In the recent era, there are various wireless applications which demand the broadcast message transmission such as road congestion notification (RCN) and intersection collision warnings (ICW) in vehicular networks, broadcasting of emergency calls for assistants in hospitals and hotels, broadcasting of region change data for conferences [1]. Rise in the practice of broadcast transmission also increases attacks and threats associated with it. Thus, there is a burgeoning interest in broadcast security field. As wireless sensor network is a resource restraint network having confined energy, so efficient adoption of energy is an essential concern in this network [2]. Security and energy are corelated to each other. If we required more security then more energy is also required, that means in the case of higher security, the nodes in the network will drain their energy expeditiously. The authentication steps involves cryptographic actions and to perform these operations more energy is required.

In this paper, we propose PEBARP, Power Efficient Broadcast Authentication and Routing Protocol, which is both secure and energy efficient. In this proposed protocol source authentication is provided by pair-wise key establishment technique and energy efficiency is achieved by using hierarchical clustering that parting the network in static clusters and disburse the power consuming tasks along with high power intermediate nodes and in the form of result extends the network life-span. In every round, PEBARP selects the intermediate node with maximal energy as the cluster-head (CH) in each cluster. PEBARP is a modified version of the BMU Routing Algorithm taking into the roles to Intermediate Nodes in WSNs [18].

BMU algorithm introduces a different type of node called Intermediate node along with sink node and sensor nodes. These intermediate-nodes view similar to sensor nodes in their physical presentation, but more energy than sensor nodes. For broadcast communication, firstly a safe connection is maintained among sink node and some intermediate nodes in hierarchical manner. After that each previously selected intermediate node establishes link with sensor nodes and stores addresses of all its adjacent sensor nodes [18]. The main difference between PEBARP and BMU is that BMU has load balancing problem because it selects the intermediate node randomly, whereas PEBARP selects intermediate node based on their energy, thus provides energy proficiency.

The remaining part of the paper is arranged as follows. Section II, III and IV describe the related work, preliminaries and proposed work respectively. In Section V and VI results and performance are discussed and in section VII conclusion part is presented.

II. RELATED WORK

Authentication of broadcast is an require service in WSNs. As sensor nodes are resource constrained, message authentication based on symmetric key cannot be directly used in sensor networks. Whereas, digital signature schemes based on asymmetric key are too expensive to be used in WSNs. As a outcome, a few broadcast authentication protocol have been suggested for resource strained wireless sensor networks.

To authenticate the signer BiBa (Bins and Balls) [3], used one time digital signature. BiBa provides precise signature and fast verification but takes larger signing- time and uses longer public key size.

Another broadcast authentication protocol called µTESLA [4] apply the key chain to compete public key cryptography with delayed key disclosure. Initially a key is chosen, and keys for subsequent rounds are accomplish by 1- way hash function. But it has many drawbacks. To increase the scalability of µTESLA, multilevel µTESLA [5] was proposed. The root concept of this protocol is to predestined and broadcast the criteria such as the key chain responsibility in place of unicast based message transmission applied in µTESLA. But, this protocol has also certain drawbacks like time synchronization requirement, more buffer storage, etc. To eliminate these drawbacks of multilevel µTesla, Batch-based Broadcast Authentication (BABRA) [6] was proposed. BABRA broadcast the packets in bunches and uses distinct keys for distinct bunches. To mitigate DoS attack presented in µTesla, Ren proposed a broadcast authentication scheme [7] that uses Merkle hash tree and identity-based signature scheme, public key scheme to provide authentication.

To provide instantaneous message verification, BAP [8] was proposed that presents two broadcast authentication protocols which are depend on primitives of symmetric-key cryptography and use cryptographic puzzles to produce effective broadcast authentication. To ensure authenticity and confidentiality of data broadcasting in single-hop networks an efficient scheme [9] uses known low complexity symmetric encryption techniques and in this scheme encryption key was changed on a per-packet basis in a testable but non-forgeable way. To defend data-centric routing protocols in sensor networks [10], Group-Key and Pair-wise key is established using local key allotment procedure. Each sensor node tries to part Pair-wise key with nodes that have little or equal height and the hierarchical structure of the sensor networks tries to maintain Group Key for every group of nodes.

To reduce communication and computation overheads in data authentication, multi hop broadcasting scheme [11] uses node collaboration and rateless information delivery mechanism. Shim et al. [13] based on Tso et al.'s identity based ideology [12] proposed an effective ID-based BA scheme, EIBAS. But Yalin et al. [16] shows this ideology has the possibility of hash collision. For secured routing in WSN, a random key pre-distribution ideology [14] was proposed in which sink node randomly chooses (n/2) nodes of a node's adjacents, called high resilient nodes, and allocate them (k+m) keys. And pending nodes get k keys. After that every node builds all feasible indirect and direct key paths to their adjacent node and uses these paths to establish pair wise key between neighbors. Mutual authentication among nodes [15] can also be provided by using a random noise matrix which is shared by sender and receiver. In this scheme, a hybrid online and offline sign-cryption procedure is also suggested which uses both the public key and digital signature encryption in a single logical tread.

BMU routing algorithm [18] uses pair-wise key arrangement [17] to provide the source authentication through intermediate nodes. Initially, a safe and sound connection is maintained between intermediate and sink nodes and then these intermediate nodes maintained contacts with sensor nodes and attain address of all its adjacent sensor nodes. But in this scheme sink node randomly selects an intermediate node and send authentication and data packets to only this intermediate node as shown in Fig. 1.

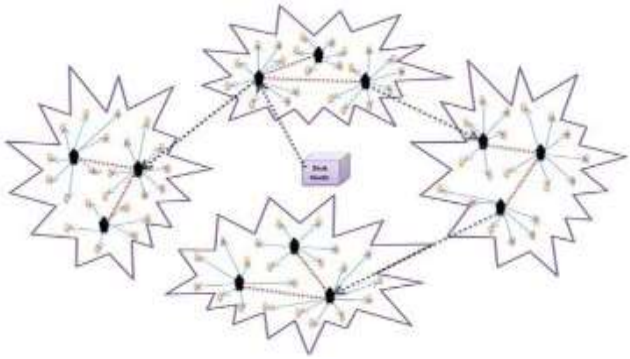

Fig.1. Broadcast Topology in BMU algorithm [18]

This selected intermediate node is responsible for forwarding all packets to the remaining intermediate and sensor nodes in the whole network. Entire load is on selected intermediate node. Thus, there is load balancing problem amidst the nodes in the network. To overcome this problem we introduce an energy effective broadcast authentication and routing protocol, PEBARP, which provide the better load balancing amidst immense power intermediate nodes, thus extends the network life-span.

III. PRELIMINARIES

Let's have a quick go through of assumptions, radio energy dissipation model and various other concepts used in this paper.

A. Assumptions

In this proposed scheme, wireless sensor network model has the following assumptions.

- Sink node (base station) is immobile.
- Entire sensor nodes are immobile and have same limited stored energy.
- Entire intermediate nodes are also immobile and have more energy and secure than sensor nodes.
- Initially all intermediate nodes have the equal energy.
- Initial deployment must be done safely.
- Clocks of all sensor nodes, all intermediate nodes and sink node must be synchronized.
- Every node either intermediate or sensor node must take or deny the packet on the support of connection identifier of the packet.

B. Radio Energy Dissipation Model

An ordinary model is assumed for the radio hardware energy dissipation in which receiver dissipates energy to implement radio electronics and sender dissipates energy to implement the power amplifier and radio electronics as shown in Fig.2.In the suggested scheme, both multi path(mp) fading (d4 power loss) and free space (d2 power loss) channel models were used, according to the distance from sender to receiver [20]. If threshold distance is greater than the calculated distance, the free space (fs) model is used; else (mp) model is used.

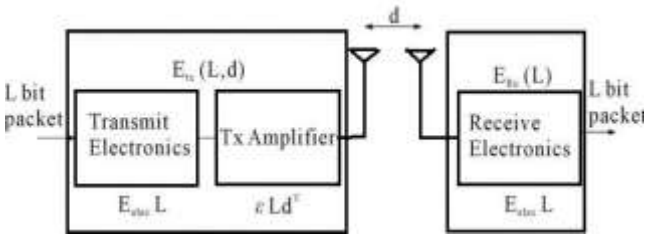

Fig.2. Radio Energy Dissipation Model

Thus, to send an *l*-bit message in a distance *d*, the radio expends

$$E_{Tx}(l,d) = E_{TX-elec}(l) + E_{TX-amp}(l,d)$$

$$= \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 , & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4 , & d > d_0 \end{cases} \quad (1)$$

where d_0 *is*

$$d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \quad (2)$$

To receive an ll-bit message, the radio expends:

$$E_{RX}(l) = E_{RX-elec}(l) = lE_{elec} \quad (3)$$

C. Definitions

1) **Random Number Generator:** This function produce a random number in the range between 1 to 100. No link exist among currently accomplish number and previously accomplish number. This function also checks whether accomplished number is positive or not. If number is not positive it reproduce a new number.
2) **Prime Number Generator:** In this function previously accomplished random number is taken as input and produce prime numbers as output. Here, function is (n^2+n+41), n is the previously accomplished random number. If the output of prime number generator is not prime then function again generates a new random number and then prime number until the generated number is not a prime number.

3) Connection Identifier: Connections among sink node, intermediate node and sensor node are identified by the 3-bit code called Connection Identifier (CI) shown in Fig. 3. CIs for the connections are given as

[000] - Sink node to Intermediate node
[001] - Intermediate node to Sensor node
[010] - Intermediate node (CH) to Intermediate node (non CH)
[110] - Intermediate node (non CH) to Intermediate node (CH)
[011] - Sensor node to Sensor node
[100] - Intermediate node to Sink node
[101] - Sensor node to Intermediate node
[111] - Sensor node to sink node

These 3-bit connection identifier shows that at any time a data packet or authentication packet is sent via a sender then only the applicable receivers will be capable to receive them.

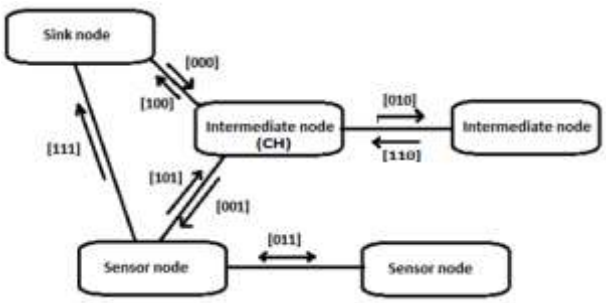

Fig.3. Connection Identifier

For example, if first three bit in the packet is [100], it means that this packet is sent from intermediate node to sink node. This information gives us an idea about that origin and destination of the packet.

4) **Dynamic circular shift function:** This (DCS) function rearranges the bit values in 8-bit tuple based on the first and last bit of the tuple. In the proposed scheme, left circular shift (LCS) is used for encryption and right circular shift (RCS) is used for decryption.

5) **Address Table***:* An address table is maintained by each intermediate node that stores the addresses of all adjacent intermediate nodes. This table is restructured whenever an intermediate node is added by a sink node.

6) **Intermediate Nodes:** Intermediate nodes are special type of nodes in the entire network. These nodes are more expensive than sensor nodes and enrich with in-built security. Thus, it is clarify that no one can access any data from these intermediate nodes over the physical tampering. These nodes seem and preceive similar to sensor nodes, thus it is hard to analyze these nodes. Intermediate nodes are primarily used to transmit data packets or authentication packets from sink node to sensor nodes and vice versa.

D. Encryption/Decryption Techniques

1) **Encryption Technique:** Let's assume that there is a connection identifier of 3 bits, 14 bits for an address, 19 bits for Value out of Function and 7 bits of function ID. Function id and function are taken from the function matrix. Connection Identifier (CI) - 010

Node's Address - 10101111001101

Function id - 1001101

Value out of Function - 1010111110001100010

In value out of function, number of bits can be added on id needed. 19 bits are taken to maintain values ranging from 0 to 50000. For encryption shown in Fig. 4, firstly concatenate all the above values as-

CI - Address - Function id - Function Value.

01010101111001101100110110101011110001100010

After that concatenation, leave the connection identifier bits apart and then divide the remaining concatenated value in various groups in which each of these groups contains 8-bits. Now apply left circular shift on each group.

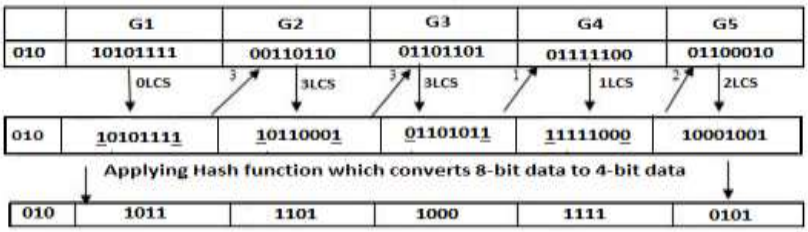

Fig.4. Encryption Technique

On group G1, perform 0 LCS all the time. For G2, take front and rear bit from group G1 (10101111) i.e. 11 in binary and equivalent to 3 in decimal. Now, perform 3 left circular shifts on G2 which results 10110001. Likewise, for G3 again consider front and rear bit of resultant G2 (10110001) which is 11 i.e. 3. Again application of 3 LCS on third group G3 results 01101011. This process continues until the last group is attained. After LCS, a hash function is applied on each group that transforms 8-bits in each group to 4-bits data. Finally resultant 23 bit encrypted packet is forwarded to directly linked nodes. Encrypted packet can be symbolized as (CI)H[DCS[Concatenate(AddressFunIDFunctionValue)]].

2) **Decryption Technique:** 23-bit packet will be collected by each receiving node. First of all we will apply reverse-hash function on collected packet that converts 4- bit data to 8-bit data. After that right circular shift function will be applied. Procedure of right circular shift is similar to that sender adopted for LCS. A minor distinction is that during encryption we execute LCS whereas during decryption RCS is executed shown in Fig.5. Thus, the resulting decrypted data are now grouped accordingly. First 3 bits specifies connection identifier, subsequent 14 bits specifies the sender's address. Consecutive 7 bits stand for function ID and remaining 19-bits stand for value out of function. This decryption procedure can be symbolized as- (CI)H[DCS[Encryptedvalue]] where Encryptedvalue stands for encrypted packet received at receiver.

IV. PROPOSED PEBARP ALGORITHM

PEBRAP is a broadcast authentication mechanism in which clusters are formed during the formation of the network. PEBRAP operates into rounds, in which each round comprises 3 phases namely Cluster formation phase, cluster head(CH) Selection phase and authentication phase. We will discuss each of these 3 phases in next sub-sections.

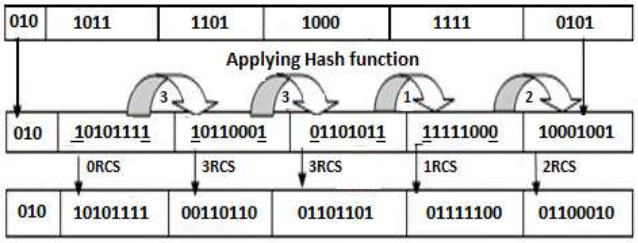

Fig.5. Decryption Technique

A. Cluster Formation Phase

As per the static clustering scheme adopted in PEBRAP, clusters are created only once at the introduction of network operation. During the cluster formation, entire network is partitioned into nemurous clusters. Each cluster comprises some intermediate nodes and many sensor nodes. Inside each cluster, each intermediate node is directly connected to other intermediate node and each sensor node is connected to nearby intermediate node as shown in Fig. 6. To broadcast data, firstly sink node establish secure connections with some selected intermediate nodes. And then these selected intermediate nodes establish secure connection with other intermediate nodes and their nearby sensor nodes. Finally each sensor node is connected to its nearby intermediate node. The entire network is connected in a tree structure form.

B. Cluster Head Selection Phase

After the clusters are formed, cluster head (CH) selection phase starts. Initially all the intermediate nodes have the same energy. In the first round, a random intermediate node inside each cluster can be elected as Cluster Head (CH) for that cluster as shown in Fig. 8. In second or more rounds, each intermediate node relays its energy level to the CH of it's respective cluster. After that CH appoints an intermediate node having maximum energy as new CH for ongoing round to perform authentication among sensor nodes and sink node. Last CH also circulates a round-start packet having new CH ID to all other nodes in its respective cluster. This packet also announces the initiation of round to all nodes (both sensor and intermediate) in its respective cluster. As each sensor node have a pre-stated time slot so switching CHs doesn't alter the cluster operation schedule.

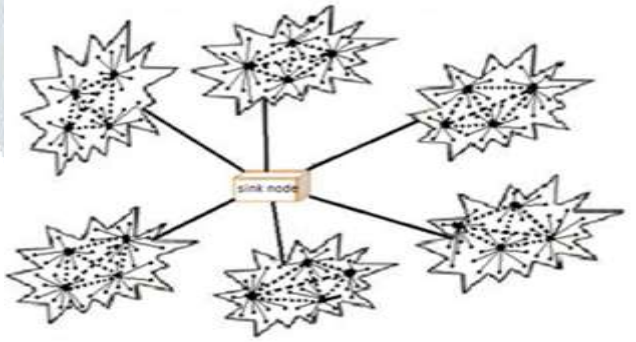

Fig.6. Cluster Formation

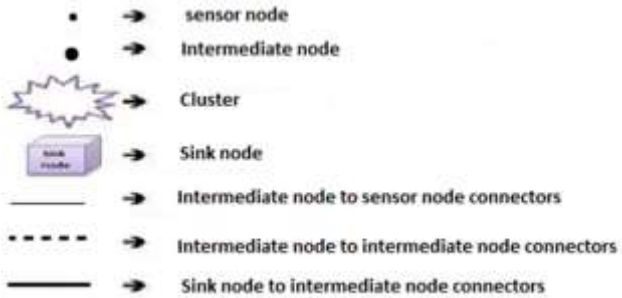

Fig.7. Symbols Used in Topology

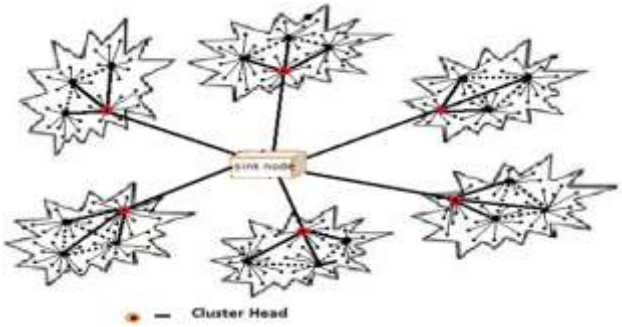

Fig.8. Cluster Head Selection

C. Authentication Phase

In authentication phase, time is divided into various time slots. Each sensor node has its specific time slot in which node sends its authentication info to its respective intermediate node. To cut down energy depletion, each non-cluster head node (either intermediate or sensor node) radio is turned off until it receives a wakeup signal from CH or its allotted transmission slot starts, but the CHs always be active all the time for accepting and transmitting the data from other intermediate and sensor nodes in the cluster. Broadcast authentication procedure works as follows-

1) Whenever sink node wants to broadcast some information to all sensor nodes, first of all it generates an authentication packet. Packet generation procedure is as follows- firstly random number generator produces an arbitrary number and using this produced arbitrary number prime number generator generates a prime number. After that, based on that prime number, a function is selected.

$$f(x) = \begin{cases} f_0(x); 007 < Prime\ no. > 691 \\ f_1(x); 743 < Prime\ no. > 2591 \\ f_2(x); 2693 < Prime\ no. > 5791 \\ f_3(x); 6047 < Prime\ no. > 10141 \end{cases}$$

For example if prime number is in the range of 7 to 691 function is selected. Each function has its own function id. Then feed this prime number into the selected function that generates value out of function. After computing Function Value sink node generates a packet of the form (CI)H[DCS[[SinkAdd][Fid FunVal]]].

Here CI = Connection Identifier
H = Hash Function
DCS = Dynamic circular shift
SinkAdd = Address of Sink node
Fid = Function Id
FunVal = Value generated from function

Sink node sends this packet to all cluster heads.

2) In each cluster, cluster head accept packet coming from sink node. Cluster Head checks CIs of incoming packet to check its origin whether it is from sink node or not. If it is coming from sink node then CH send a wake up signal to all the non CH nodes connected to it. After that it makes appropriate changes in the packet, generate multiple copies of packet [CI][CHAdd]H[DCS[SinkAdd] [Fid FunVal]] and send to all connected sensor nodes and other intermediate nodes in their respective cluster.

3) After receiving a wakeup signal sensor node and intermediate nodes (other than cluster head) come into active state and receive the packet. Intermediate nodes do the same as step 2, verify the CH address, generate packet of the form [CI][InodeADD]H[DCS[[SinkAdd][Fid FunVal]]] and send that packet to all sensor nodes connected to them. All sensor nodes, that receive a packet from CH or other intermediate nodes, verify the intermediate node address and then check packet's authenticity. Authentication verification procedure at sensor node is same as BMU algorithm [1]. After authentication of packet, sensor node also generates a packet using different random number. Packet is of the form [CI]H[DCS[[SensorAdd][Fid FunVAl]]] and send this packet to that intermediate node (CH or non CH) from which it receives the packet. Sensor nodes take that address from the incoming packet.
4) On receiving packet from sensor nodes**,** first of all intermediate nodes (CH or non CH) verify the authenticity of packet and after the successful authentication it stores sensor node address in its Volatile Session Address Collector (VSAC).
5) Sink node sends broadcasting information to all CHs. All CHs convey this information to all connected intermediate nodes. All intermediate nodes (CH or non CH) forwards this data only to those sensor nodes whose address in the volatile session address collector.

V. SIMULATION STUDIES AND RESULT

The performance of PEBRAP protocol is being evaluated through MATLAB [19] simulation. All nodes are randomly deployed within the network area. In PEBARP simulation, we presume that all node clocks are already synchronized. PEBARP simulation was executed in ideal channel environment and also in realistic channel environment. The network parameters such as network size, number of nodes, number of clusters, base station location and energy parameters such as initial energy of nodes, energy model parameters used in this simulation study are specified in TABLE I.

Table 1. Simulation parameters

Parameters	Values
Network size	(0,0) to (100,100)
Number of nodes	100
Base station location	(50,50)
Number of clusters	4
Number of intermediate nodes	12
Initial Energy of sensor nodes	0.2
Initial Energy of intermediate nodes	0.4
Eelec	50×0.000000001
Efs	10×0.000000000001
Emp	0.0013×0.000000000001
EDA	5×0.000000001

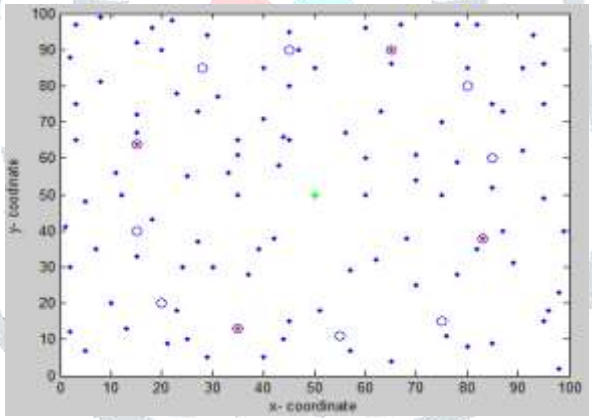

Fig.9. Cluster heads for round 1

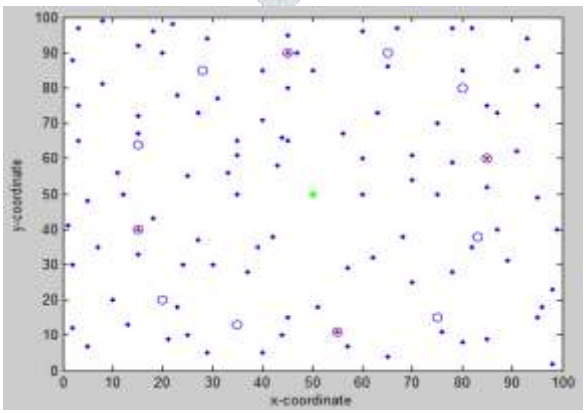

Fig.10. Cluster heads for round 2

In Fig. 9. and Fig. 10.,

- - Represents sensor node
- - Represents intermediate node

- Represents intermediate node as cluster Head
- Represents sink node

Fig. 9 and Fig. 10 shows the Cluster Heads for round 1 and round 2. CHs in every round changes according to the energy level of the intermediate nodes. CH of any cluster in every round is the intermediate node of that cluster that has the maximum energy in that round. Thus, this clustering scheme provides better load balancing compared to BMU algorithm.

VI. SECURITY AND PERFORMANCE ANALYSIS

Evaluation of the suggested scheme is carried out according to two main criteria- security and energy efficiency. They both are contrary to each other. If we are taking energy efficiency under consideration then we can't give the assurance for better security and vice versa.

A. Security

This suggested protocol has been evaluated to gain the appropriate level of security. Considering the suggested authentication protocol, nodes confirm authentication through pair-wise key establishment where 2-authenticating parties are authenticated mutually by each other. Our newly devised method is capably enough to serve complete resilience to network across to node captures. The primary key points is that security of our method go around to 2- key criteria those are prime numbers used and function equipped on discrete nodes. And both the criteria are selected by senders and receivers on the randomly basis this is the main thing so it is also hard to get spoofed.

B. Energy Efficiency

Effective use of energy is a major issue because WSN is a resource restraint network and it have limited energy. This suggested algorithm uses hierarchical clustering to divide the network into various clusters. Each cluster has some intermediate nodes and many sensor nodes. Intermediate nodes have more energy than sensor node and they provide the communication between sink node and sensor nodes. In each round, inside each cluster an intermediate node that has maximum energy elected as cluster head. Thus, in each round cluster heads are changed depending upon the remaining energy of the intermediate nodes in each cluster. Hence, provides better load balancing. Sink node sends the authentication data packet to the cluster heads. Then these cluster heads send this packet to its adjacent sensor nodes. Fig. 11 and Fig. 12 show the number of dead intermediate nodes and alive intermediate nodes against rounds.

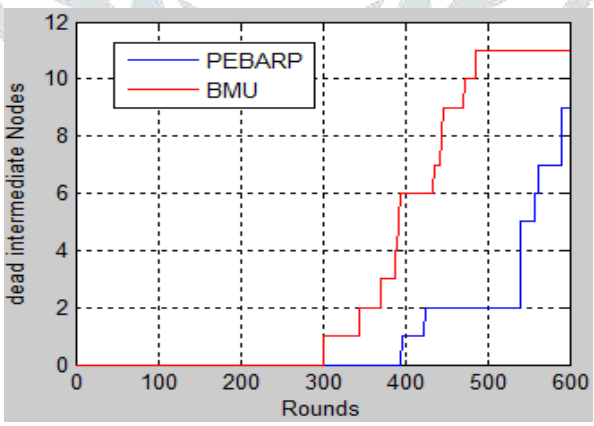

Fig.11. Number of dead intermediate nodes over rounds

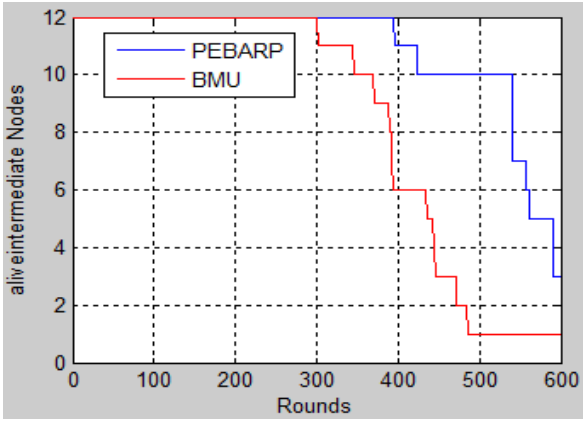

Fig.12. Number of alive intermediate nodes over rounds

PEBRAP executes better when compare to other protocols like BMU routing algorithm, in view of our protocol CHs are picked in terms of the energy level of the intermediate nodes but in BMU intermediate node is selected on the random basis by the sink node and this intermediate node is responsible for forwarding the packet to the whole network. Here, entire load is on that selected intermediate node. Fig.11 and Fig.12 clearly show that our protocol is enhanced from BMU in terms of energy consumption.

C. Computational, Transmission and Storage Overheads

In this proposed scheme, simple computations are performed for encryption and decryption of packet. Thus, there is very less computational overhead. Transmission overhead is defined by the time elapsed in carrying of data packets. Its evaluation supports in clarifying a division of security complications. To achieve this goal, we analyze the extra expenses at three extensive places they are sink node(base station),sensor nodes and intermediate nodes. Extra expenses of the procedure is mainly shortened becuse of 2-3 hop count depth of the network. If we properly studied the topology we can conclude that all node (sensor node or intermediate node or sink node) has to transmit its data packet to 1 hop number depth out or in of the network. There is no role of key chain in this proposed scheme, because in the proposed scheme dynamically generated keys are used which are discarded after authentication. Thus, there is no storage overhead of key-chain storage.

VII. CONCLUSION

We introduce PEBARP, an energy-efficient broadcast authentication protocol which parting the network into static hierarchical clusters, utilizes temporary-CHs to share the energy load between high power intermediate nodes; thus enhance the network life-span. The proposed broadcast authentication and routing algorithm is one of the basic approaches to broadcast some urgent data packets. In this scheme source authentication has been done securely using the encryption decryption technique proposed. PEBRAP performs better than BMU routing algorithm, since in our protocol cluster heads are selected based on the energy level of the intermediate nodes but in BMU sink node randomly selects an intermediate node to perform authentication process. Future work demands introduction of dynamic clustering to form the clusters instead of static clustering.

References

[1] K. Grover, A. Lim. A, "Survey of broadcast authentication schemes for wireless networks," Ad Hoc Netw., 2014, in press.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," Computer Networks , 2002, 38: 393–422.

[3] Perrig A, "The biba one-time signature and broadcast authentication protocol," In proc. 8th ACM conference on Computer and Communications Security. New York, NY, USA: ACM, 2001, pp. 28-37.

[4] Perrig A., Szewczyk R.,Wen V., Culler D., Tygar J. D., "SPINS: Security protocols for sensor networks," Wireless networks, 2002, 8(5): 521-534.

[5] Liu D, Ning P., "Multilevel μ tesla: Broadcast authentication for distributed sensor networks," ACM Trans Embed Comput Syst, 2004,3: 800-836.

[6] Yun Z; Yuguang F., "BABRA: Batch-based Broadcast Authentication in Wireless Sensor Networks," In Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE, pp.1-5.

[7] Kui R, Wenjing L, Kai Z, Moran P.J., "On Broadcast Authentication in Wireless Sensor Networks," in Wireless Communications, IEEE Transactions on, November 2007, vol.6, no.11, pp. 4136 - 4144.

[8] Patrick S, Srdjan C., David B., "BAP: Broadcast Authentication Using Cryptographic Puzzles," In Applied Cryptography and Network Security, 5th International Conference, ACNS, Springer Heidelberg, 2007, pp. 401-419.

[9] Shaheen,J.; Ostry, D.; Sivaraman, V.; Sanjay Jha., "Confidential and Secure Broadcast in Wireless Sensor Networks," In Personal, Indoor and Mobile Radio Communications, IEEE 18th International Symposium on, 2007, pp.1-5, 3-7 Sept. 2007.

[10] Guermazi A., & Abid, M., "An efficient key distribution scheme to secure data-centric routing protocols in hierarchical wireless sensor networks," 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), Procedia Computer Science, 2011, 5, pp. 208–215.

[11] Ayday, E., & Fekri, F., "A secure broadcasting scheme to provide availability, reliability and authentication for wireless sensor networks," Ad Hoc Networks, 2012, 10(7): 1278–1290.

[12] R. Tso, C. Gu, T. Okamoto, E. Okamoto., "Efficient ID-based digital signatures with message recovery," In Proceedings of CANS ' 07, LNCS 4856, Springer-Verlag, 2007, pp. 47–59.

[13] K.-A. Shim Q1 et al., "EIBAS: An efficient identity based broadcast authentication scheme in wireless sensor networks," Ad Hoc Networks, 2012.

[14] Senthil kumaran, U., & Ilango., "Key pre-distribution scheme for randomized secured routing in wireless sensor networks (WSN'S)," Journal of Theoretical and Applied Information Technology, 2013, 51(1).

[15] U. Senthil kumaran, P. Ilango., "Secure authentication and integrity techniques for randomize secured routing in WSN," in Springer Science+Business Media, New York, 2014.

[16] Yalin Chen, Jue-Sam Chou., "Comments on EIBAS: an efficient identity broadcast authentication scheme in wireless sensor network," in ICAR, 2015.

[17] Sanjay K, Singh RK., "Pair-Wise Key Establishment Using Random Number and Distinct Random Functions in WSNs," IACC100728: Proceedings of the 4th annual international conference on Mobile computing and networking, 2013, pp. 863-869.

[18] Kumar S, Singh RK., "BMU Routing Algorithm through Smart Role of Intermediate Nodes in WSNs," J Comput Sci Syst Biol., 2015, 8: 104-111.

[19] MATLAB, http://in.mathworks.com/downloads/web_downloads.

[20] W. B. Heinzelman, A .Chandrakasan, and H. Balakrishanan., "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, Oct.2002, pp.660-70.


JETIR