ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Trustworthy Routing Protocol for WSN

M Swathi Mithran Sushama, C.Suryawanshi

Dept. of Computer, SCOE, Pune, India

Assistant Professor, Dept. of Computer, SCOE, Pune, India

ABSTRACT*:* In wireless sensor networks (WSNs), the present bunch based information accumulation procedure expends more vitality. Additionally the secured information transmissions are essential for upgrading the information confirmation and secrecy. Keeping in mind the end goal to conquer these issues, in this review, In this paper, we provide detailed analysis on the relations between clustering and routing, and then propose a Ambient Trust Sensor Routing (ATSR) protocol for reliable and efficient data collection in large-scale wireless sensor network. ATSR adopts the back off timer and gradient routing to generate connected and efficient inter-cluster topology with the constraint of maximum transmission range. The relations between clustering and routing in ATSR are further exploited by theoretical and numerical analysis. The results show that the multi-hop routing in ATSR may lead to the unbalanced cluster head selection. Then the solution is provided to optimize the network lifetime by considering the gradient of one-hop neighbor nodes in the setting of back off timer. Theoretical analysis and simulation results prove the connectivity and efficiency of the network topology generated by ATSR.

KEYWORDS*:* WSN, data aggregation, clustering process, data security, packet delivery, energy consumption, packet drop, transmission overhead.

I. INTRODUCTION

The wireless sensor network includes small and less cost sensing devices together with wireless radio transceiver for examining the environment. It involves the data gathering and transmitting the information to one or more sink nodes. The main advantage of this network is that it does not require any infrastructure or external supply for data gathering. The main applications of WSN are wild habitat monitoring, forest fire detection, building safety monitoring, military surveillance and so on.

The characteristics of WSN, which have resulted in challenging issues, are as follows:

I. Sensor nodes are exposed to maximum failures.
II. Sensor nodes utilize the broadcast communication pattern and possess severe bandwidth restraint.
III. Sensor nodes hold scarce quantity of resources.

Owing to the limited availability of resources, the amount of data transmission needs to be minimized. This in turn will enhance the network lifetime and bandwidth utilization. This can be achieved through data aggregation.

The process of collecting the data from various sources followed by redundancy elimination thereby minimizing the transmission count is termed as data aggregation. This process leads toenergy conservation. Moreover, the inherent redundancy in data gathered from the sensor node can be removed through the process of in-network data aggregation. This is mainly executed for extracting application specific information. However, in hostile environment, the aggregated data need to be protected from various attacks for attaining the data confidentiality, integrity and authentication. Hence, security plays a major role in data aggregation [1].

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

II. SECURITY REQUIREMENTS

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

In hostile environment of WSN, security is a key issue, whose requirements are discussed below

A. *Data Confidentiality*

The process of safeguarding the transmitted data from passive attacks corresponds to data confidentiality. The process of securing the data from illegal user is the most challenging task. This can be solved by using an encryption technique such that only the intended user with appropriate key can unlock and read the data.

B. *Data Integrity*

The compromised source nodes or aggregator nodes are prevented from altering the final aggregation value by data integrity. Since sensor nodes lack expensive tampering resistant hardware, they can easily be compromised. Moreover, this tampering-resistant hardware will not be reliable every time. A compromised node can modify, copy or discard messages[2].

C. *Data Accuracy*

The aggregated data need to be provided with more accuracy. As high accuracy requires more memory and high energy, a trade-off among the data accuracy and aggregated data size should be taken into consideration. Availability: This means that the network services need to be available even during the internal and external attacks namely denial of service (DoS) attack. The technique that involves in offering availability makes use of extra communication facilities among the nodes or central access control system to ensure successful delivery of every message to its recipient.

D. *Reply Attack*

If an attacker records some traffic from the network without any content knowledge and replays those in the later period to mislead the aggregator, then the aggregation results consequently obtains affected.

E. *Node Compromise Attack*

During this attack, the adversary arrives at the node and extracts the data stored in it. With respect to the data aggregation application, once the node has been captured by this attack, the entire secured information can be extracted. This attack is also called as the supervision attack.

F. *DoS Attack*

This is most commonly referred to as jamming attack that transmits the radio signals for obstructing the radio frequencies used by WSN. The increase in adversary capacity can affect the major portion of the network. During aggregation, this attack causes the aggregator node to prevent the data from obtaining transmitted to higher levels.

G. *Sybil Attack*

This type of attacker has a capacity to offer more than one identity within the network. It affects the data aggregation in the following ways:

1. The attacker initially generates multiple identities for creating additional votes during aggregator election phase and chooses a malicious node to be the aggregator. If the adversary is able to generate numerous entries with different readings, the aggregated result obtains corrupted.
2. An adversary can launch a Sybil attack and create n or more identities, thus making the base station to accept the aggregation results.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

H. ***Stealthy Attack***

This attack involves the injection of false data into the network without revealing its presence.In a data aggregation concept, the injected false data value can lead to a false aggregation result.

III. CLUSTER BASED DATA AGGREGATION

In cluster-based data aggregation, sensor nodes are subdivided into clusters. In each cluster, a cluster head is elected in order to aggregate data locally and transmit the aggregation result to the base station. Cluster heads can communicate with the sink directly via long range radio transmission. However, this is quite inefficient for energy constrained sensor nodes. Thus, cluster heads usually form a tree structure to transmit aggregated data by multi hopping through other cluster heads which results in significant energy savings. *Fig. 1* presents an example of Cluster- based data aggregation[6].

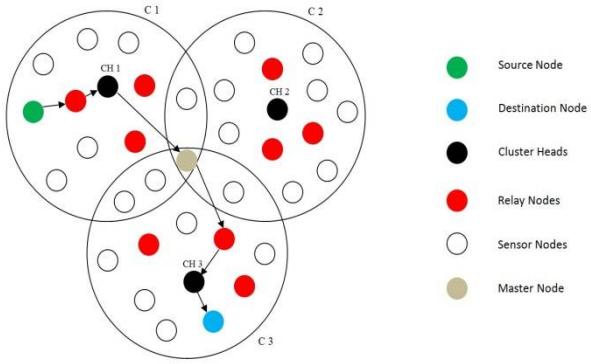

Fig. 1 : Cluster Based Data Aggreagation

Maximum Lifetime Routing in Wireless Sensor Networks In wireless sensor networks where nodes operate on limited battery energy, the efficient utilisation of the energy is very important. One of the main characteristics of these networks is that the transmission power consumption is closely coupled with the route selection. The energy efficiency has been considered in wireless ad hoc network routing, but the conventional routing objective was to minimise the total consumed energy in reaching the destination.

The new problem formulation has revealed that the minimum total energy routing is not suitable for network-wise optimum utilization of transmission energy. The significant improvement can be made by the new routing algorithm in terms of maximising the system lifetime, which can also be interpreted as maximising the amount of information transfer between the origin and destination nodes given the limited energy. The routing algorithm is a shortest cost path routing whose link cost is a combination of transmission and reception energy consumption and the residual energy levels at the two end nodes. The simulation results are close-to-optimal performance most of the time with both the fixed information-generation rates and some arbitrary information-generation process of a moving target detecting scenario in wireless sensor networks [8].

IV. LITERATURE SURVEY

In literature, the problem and the previous techniques of the cluster-based data aggregation in wireless sensor networks Aggregation in Wireless Sensor Network ", 2010 IEEE International Conference on Computational Intelligence and Computing Research ..A data aggregation algorithm is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks (WSN) offer an increasingly Sensor nodes need less power for processing as compared to transmitting data. Data aggregation protocols aims at eliminating redundant data

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

transmission and thus improve the lifetime of energy constrained wireless sensor network. High-Confidence Transport and Asset Tracking Healthcare Smart Home.

Sankardas Roy et al.[3] Diffusion approach secure against attacks in which compromised nodes contribute false sub aggregate values. In particular, we present a novel lightweight verification algorithm by which the base station can determine if the computed aggregate (predicate Count or Sum) includes any false contribution. Thorough theoretical analysis and extensive simulation study show that our algorithm outperforms other existing approaches. Irrespective of the network size, the per-node communication overhead in our algorithm is O (1). Wild habitat monitoring, Forest fire detection and Military surveillance.

Priyanka S. Fulare et al.[4] In wireless sensor networks, compromised sensor nodes can inject false data during both data aggregation and data forwarding. In this paper discuss how the data is being remained confidential between sink and destination by using Data authentication method for securing the data in wireless sensor network. 1.Vehicular movement lightning condition.

Hevin Rajesh et al.[5] Fuzzy based secure data aggregation technique which was having 3 phases. In its first phase, it performs clustering and cluster head election process. In the second phase, within each clusters, power consumed, distance and trust values were calculated for each member. In the third phase, based on these parameters, fuzzy logic technique was used to select the secure and non-faulty node members for data aggregation. Electromechanical devices like temperature Measurement and Humidity Measurement.

Hani Alzaid et al.[6] In this paper discus the security issues such as data integrity, confidentiality, and freshness in data aggregation become crucial when the WSN is deployed in a remote or hostile environment where sensors are prone to node failures and compromises. Design a conceptual framework to minimize the security issues. Measurement of physical parameters such as temperature, pressure, or relative humidity.

B. A. Makinet al.[7] This paper proposes a trust-based secure data aggregation protocol for WSN. It does not involve any centralized infrastructure. It uses Combined Trust Values (CTVs) to favour packet forwarding for each node. In this scheme, each sensor node has a CTV which is based on the trust evaluation factors, such as identification, sensing data and consistency. Based on these factors, one can identify malicious or compromised nodes, and filter their data from the networks. Each aggregator determines a Message Authentication Code (MAC) value for the aggregated data and finally all the aggregated data reach the sink node. By verifying the MAC value of the aggregators, the sink identifies and eliminates the misbehaving aggregators. The simulation results show that the proposed protocol achieves good delivery ratio and throughput.

H. Miao et al.[9] Based on LEACH Protocol, an improved LEACH Protocol (LEACH-H) is based on Genetic Algorithm(GA) in this paper. The weight values of the three influencing factors the current residual energy of nodes, the number of the neighbour nodes and the distance between nodes and base station are used as its optimization variable. The maximum lifetime of the first and half of the nodes is used as the optimization objective. Finally, the LEACH protocol before and after improvement are applied to the prefabricated substation. The sensor nodes are used to collect equipment operating parameters and substation environmental parameters. LEACH-H and LEACH protocol are used separately for data transmitting. The simulation results show that the lifetime of the first and half of the nodes of LEACH-H protocol is longer than the original LEACH protocol, and the performance of the network is improved.

Clustering Mechanism of LEACH Protocol

The selection method of cluster head in LEACH protocol is that the sensor node generates a random number between [0,1], if the random number is less than or equal to the node's threshold *T (n)*, the node is elected as the head node of the cluster.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

A. The Problems of LEACH Cluster Mechanism

The cluster head election process is completely depended on the random number in the node generates, for other attributes of the nodes, such as the current residual energy, location are not considered, which has the following problems:

1) Without considering the residual energy of nodes when select cluster head, this may cause low-energy node is selected as a cluster head, which makes the node energy exhausted quickly.

2) The location of the node is not considered when cluster head is distributed, and cannot guarantee the uniform distribution of cluster head. It may cause some cluster heads are densely distributed, or cluster heads are too sparse, even no cluster head in certain areas.

B. Improvement of Cluster Mechanism

In view of the problem in LEACH protocol, take the energy and the position of nodes into account to optimize the selection mechanism. The improved algorithm introduces three parameters include energy, the node's number of neighbours, the distance between node and base station to correct threshold.

V. SYSTEM ARCHITECTURE

We have proposed a Genetically Derived Secure Data Aggregation in WSN. Initially, the CHs are chosen based on the node connectivity, which acts as a data aggregator (DAG). Then, the clustering process is executed using the genetic algorithm. This technique and thereby enhancing the network lifetime. When the cluster member wants to transmit the data to the aggregator, a data encryption technique are utilized. The crypto module (CyM) utilized offers confidentiality to the data packet (DP), thus ensuring the authenticity and integrity of the sensed data.

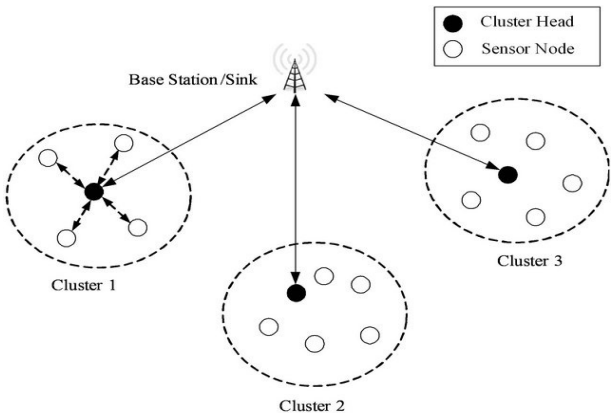

Fig. 2 : Proposed Cluster Creation and Transmission Process

Cluster Formation :

Fig. 2 describes the cluster creation process and transmission between source and destination node. At the end of each TS network nodes verifies sensed data and broadcast messages to nodes within given Cluster Distance (CD) for cluster creation. Cluster creation uses the Relay Node (RN) and CD to group the sensor in same cluster. Upon accepting the broadcasted message each node verifies the value of RN. If its value is within RN it stores in its memory and compares CD with each node's distance. If the distance between nodes is same or less to CD and sensed value is within given RN then those group of nodes forms a cluster. The nodes NID which are related they will not broadcast message for cluster creation. Nodes which are not participate in cluster creation process based on *RN* and *CD.*

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Cluster Head Selection :

Upon completion of cluster creation task each node has its cluster member NID, Node Location (NL), NTE and Sink Location (SL), battery power information in its memory. The node having maximum energy will calculate minimum distance of each node within range known as Cluster Head (CH) and broadcast CHID to other network nodes. It also measures the node having minimum distance from the sink called Cluster Head Transmission (CHT) and broadcast CHTID to CH. This node (CHT) will be used to transmit data toward sink if remaining CH energy is not sufficient for data transformation after measurement. Once each node knows it's CH it transmits data to CH. Cluster head transmit processed information to the sink, this communication is single hop communication, means it make direct communication with sink.

Boundary Node Formation :

A dynamic cluster will be built when the target comes close to the boundaries of multiple clusters. A demanding task issue is how the system finds the scenario when the target is approaching the boundaries, especially in a fully distributed way. We use boundary nodes to solve this issue in a fully distributed way.

Multi Hop selection :

1) The multi-hop planar model :

A CH node transmits data to the BS by forwarding its data to its neighbour nodes, in turn the data is sent to the BS. We have proposed an energy efficient routing algorithm for hierarchically clustered WSNs and it is suitable for the proposed secure data transmission protocols.

2) The cluster-based hierarchical method :

The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS.

Advantages of Cluster Based Topology

When we use cluster based on demand dynamic routing protocol for moving target tracking in a given region in wireless sensor network. This protocol grows the scalability of a sensor network. Throughout energy consumption of the nodes is reduced, leading to prolonged network lifetime. Sensor nodes organized into cluster network borrow itself for perfect data aggregation, which in turn results in better utilization of the channel bandwidth. Cluster-based routing take good assurance for many-to-one and one-to-many communication samples those are regnant in sensor networks. With the help of this protocol we trace out the exact position and path travelled by target at a given instant of time without any mistake.

1) ADVANTAGES OF PROPOSED SYSTEM

A. Highly minimizes the energy utilization.
B. ***Ensures data security and reduces the transmission overhead.***

VI. SYSTEM ANALYSIS

Algorithm: Generate an RSA key pair.
Input: Required modulus bit length, k.
Output: An RSA key pair ((N,e), d) where N is the modulus, the product of two primes (N=pq) not exceeding k bits in length; e is the public exponent, a number less than and co prime to (p-1)(q-1); and d is the private exponent such that $ed \equiv 1 \pmod{(p-1)(q-1)}$.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Select a value of e from {3, 5, 17, 257, 65537}
repeat
p ← gen_prime(k/2)
until (p mod e) ≠ 1
repeat
q ← gen_prime(k - k/2)
until (q mod e) ≠ 1
N ← pq
L ← (p-1)(q-1)
d ← mod_inv(e, L)
Return (N, e, d)

Head Selection

Input: Cluster set with nodes.
Output: Ch selection with remaining sensor node.
Step 1: select all nodes as initial population.
Step 2: Select evaluation set
Step 3: Apply crossover on similar power nodes.
Step 4: Apply mutation on each sensor node.
Step 5: Apply fitness on all nodes power
Step 6: select best node using routlet wheel selection.
Step 7: Check GA evaluations
Step 8: Select final max energy node as CH node.

Mathematical Model
The system has classified into the different sets like below
Sys={inp, process, out, analysis}
Inp= {D1,D2……Dn}
That is the set of input data chunks

$$EncData \sum_{n=1}^{m} Enc(D) \dots Enc(Dn)$$ ------- (1)

Equation (1) shows the data aggregation as well as data encryption process.
Data=∑ D[i] ----- (2)
Equation (2) shows the get the data from each node

$$Plaindata \sum_{n=1}^{m} Dec(D) \dots Decc(Dn)$$ ------ (3)

Equation (2) shows the data aggregation of cipher data on receiver phase with decryption process.
Success condition
If(inp != Null)
Failure condition
IF(D == NULL)

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

VII. Results and Discussion

In order to evaluate the performance of system performed. The network architecture considered is the following:

[1] A fixed base station (sink node) is located away from the sensor field.
[2] The sensor nodes are energy constrained with homogeneous initial energy allocation.
[3] Each sensor node senses the surroundings at a fixed rate and at all times its data to send to the base Station (data are sent if an event occurs).
[4] The sensor nodes are assumed to be stationary. However, the protocol can also support

We compare the proposed system results with different existing system. Below table shows the comparison analysis of proposed system with some existing system

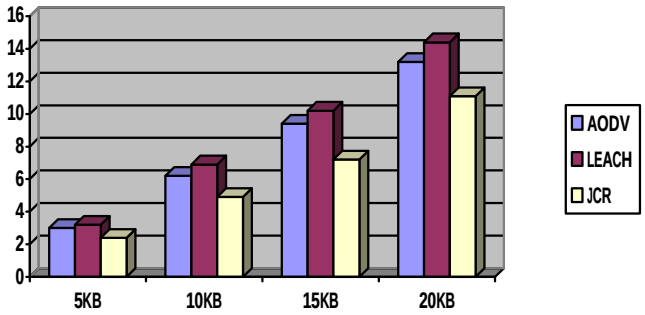

Fig 3: System Comparison proposed vs Existing (Milliseconds)

We consider energy evaluation for transmission which will conserve the node energy at the time of transmission, the system will select efficient path for communication with neighbour node at same time remaining network will sleep node.

VIII. Conclusion

We have proposed a joint clustering and routing (JCR) protocol to provide reliable and efficient data collection in large-scale WSN. The random backoff and gradient routing schemes are adopted in ATSR to execute the cluster head selection and multi-hop routing simultaneously with low overhead. Theoretical analysis and simulation results prove that ATSR can provide connected and efficient inter-cluster topology with limited transmission range. Moreover, the backoff timer in ATSR can be carefully tuned to balance the energy consumption and prolong the network lifetime., we show that the proposed technique minimizes the energy consumption, ensures data security and reduces the transmission overhead.

References

[1] Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network", 2010 IEEE International Conference on Computational Intelligence and Computing Research.
[2] B. A. Makin and D. A. Padha, "A Trust-Based Secure Data Aggregation Protocol for Wireless Sensor Networks," pp. 7–22, 2010.
[3] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 3, JUNE 2012.
[4] Priyanka S. Fulare, Nikita Chavhan, "False Data Detection in Wireless Sensor Network with Secure communication", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume-1, Issue-1, 2011.
[5] Hevin Rajesh, D. and B. Paramasivan, "Fuzzy Based Secure Data Aggregation Technique in Wireless Sensor Networks" Journal of Computer Science 8 (6): 899-907, 2012
[6] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey", Information Security Institute Qeensland University of Technology.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

[7] Ozdemir S, Xiao Y, "Secure data aggregation in wireless sensor networks: A comprehensive overview", Comput. Netw., 2009, 53, (12), pp. 2022–2037.
[8] ae-Hwan Chang, Leandros Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 12, NO. 4, AUGUST 2004.
[9] H. Miao, "Improvement and Application of LEACH Protocol based on Genetic Algorithm for WSN," pp. 242–245, 2015.