A Unique Location-Key pair based Security for Wireless Sensor Network

R. Amuthavalli and Dr. R. S. Bhuvaneswaran

Wireless Sensor Networks are platform independent systems that can be deployed in any emergency situations such as Monitoring, Surveillance and Military applications. On account of this the nodes can be deployed in the network at random. These are dynamic nodes and the distance between nodes is long. Hence they transmit data through a multi-hop. These nodes are not trustworthy due to their dynamic, self-organized nature and can accommodate themselves in any existing infrastructures. Hence it is imperative for the network to monitor every new node that joins the network or any node that interacts with other existing node, is a trusted node and not a malicious node. The existing studies have introduced various approaches and algorithms for security in wireless network. In this paper we discuss a dynamic random key pair matching algorithm based on node arrangement mechanism for secured node placement in the network. The proposed work is categorized into two tasks; the first task is to determine the secure node location and the second task is secure node placement. For node location determination the value of the node is taken as the key pair and for node placement clustering method is used which also gives energy efficiency. Ensuring security for each node implies that the communication among the nodes cannot be misused by malicious node. The efficiency of the network is also improved by minimizing the energy loss in clustering methods. The simulation results show that the proposed approach is efficient than the existing approaches.

INTRODUCTION

Wireless Sensor Network (WSN) is a collection of sensor nodes that can communicate with each other via wireless links and can self-organize to accommodate itself to the existing infrastructure. The nodes are random and dynamic, so the topology may change rapidly and unpredictably. The data packet sending and receiving is executed by the nodes themselves either individually or collectively. Based on application of the network and node structure, the data transmission energy can be saved. The network comprising of mobile nodes is divided into two types namely open network and closed network (H. Miranda and L. Rodrigues, 2002). In closed network the nodes are used in emergency situation, but in the open networks the nodes are used for global connectivity. In these situations, the energy consumption as well as the security is the two main factors to be considered.

In this paper, we are presenting a novel algorithm that implements security of nodes in the network as well as provides energy efficiency. The novel algorithm employs unique node based clustering with location based key matching. Though, some resources are expended quickly as the nodes also contribute towards various other network roles. [Kejun Liu, 2003] discuss in their paper that energy measures are the most significant metrics in a mobile environment. A separate mobile node may attempt to benefit from other nodes, but refuse to share its own resources. The paper concludes that the security is obtained through Node Key assignment and Clustering can be obtained by a new clustering method.

Related Work:

(Kejun Liu, 2007) proposed the 2ACK system that helps as an add-on method for routing systems to sensor routing misbehavior and to alleviate their opposing effect. The key impression of the 2ACK system is to send two-hop response packets in the reverse direction of the routing path. In order to decrease extra routing overhead, only a portion of the received data packets are acknowledged in the 2ACK scheme. (S.N.Chobe, 2004) proposed the 2ACK system to help routing systems to sensor routing misbehavior and to alleviate their opposing effect. The key impression of the 2ACK system is to send two-hop response packets in the reverse direction of the routing path. In order to decrease extra routing overhead, only a portion of the received data packets are acknowledged in the 2ACK scheme. (S.N.Chobe, 2004) proposed the 2ACK system to help routing systems to sensor routing misbehavior and to alleviate their opposing effect. The key impression of the 2ACK system is to send two-hop response packets in the reverse direction of the routing path. In order to decrease extra routing overhead, only a portion of the received data packets are acknowledged in the 2ACK scheme.

Corresponding Author: R. Amuthavalli, Assistant Professor, MCA Department, SSN College of Engineering, 603110, Chennai, India.
E-mail: amuthavallir@ssn.edu.in
2013) proposed a new scheme called 2ACK is used where the 2ACK scheme is to send two-hop acknowledgment in opposite direction to routing path. In 2ACK scheme, to reduce extra routing overhead, only a few of the received data packets are acknowledged. (Jakobsson, M. and Hubaux, 2003) said the idea of nuggets is used as payment. There are two prototypes1) Packet trade type 2) Packet purse type. In the Packet Trade type, in-between node purchases the packet from the earlier node for some nuggets and retails it to the following node for more nuggets (Jakobsson, M. and Hubaux, 2003).

(Marti, S. and Giuli, 2007) detect and eliminate the malicious node the watchdog and the pathrater mechanism are used. The Best-effort Fault-Tolerant Routing (BFTR) system also employs end-to-end ACKs (Yuan XueAnd Klara Nahrstedt, 2004). S. D. Khatawkar, 2011 discussed about the various systems was discussed that serves as an add-on technique to detect routing misbehavior and to mitigate their adverse effect. But applying monitoring mechanism to each individual nodes and validate the node while communication brings more effect than other techniques. (V. Manjula and C. Chellappan, 2011) proposes a technique Randomized and Trust based watcher judgment strategy for duplication attack detection mechanisms in wireless sensor networks(RTRADP) with trust factor.

(Subhasis Bhattacharjeet, Al, 2013) proposed a novel mechanism used to verify the neighbor nodes and select a secured shortest path to transfer the data in secured manner. (Jianguo SHAN, 2013) represents about the energy saving by LEACH protocol in various kind of WSN topology. The necessity for safety in LEACH protocol has motivated many scholars to design protected versions of this protocol and to create it resilient against insider and outsider attackers. (Mohammad Masdari, 2013) discussed about the current state-of-the-art secure LEACH schemes that are proposed in literature. (Hiren Kumar Deva Sarma, 2011) said a novel secure routing protocol is projected for wireless sensor networks in which sensor nodes as well as the base station are mobile. The protocol achieves security property through symmetric key cryptography and threshold key cryptography.

**Problem Statement:**

On account of the mobile, dynamic and self-organizing characteristic of the wireless sensor network, it is imperative that appropriate security measure are employed in order to ascertain whether the nodes are trustable nodes are not. These security measures ensure that the communication among the nodes is not misused by malicious node or any node from outside the network. The proposed paper assigns a secret key for all the nodes and places the nodes in such a manner that there is uniform communication among the nodes. This improves the QoS parameters such as packet delivery ratio, throughput and energy.

**Existing Approach:**

The node misbehavior can be detected and controlled by different techniques such as Intrusion Detection System (IDS) (Isha V. Hatware, 2012), Cooperative Intrusion Detection, watchdog and path rater. These are more efficient than other general techniques. In the existing system the identification of misbehaving nodes in ad-hoc networks is critically important to detect security attack in the network. The two types of misbehaving nodes detected and identified in the existing system namely selfish and malicious nodes are taken into consideration.

**Proposed Approach:**

The existing approaches employed varied IDS techniques for providing security in WSN. In this paper, the proposed approach provides energy loss minimization and security using a agglomeration mechanism. This agglomeration mechanism could be a new methodology integrated with security at the node level. The node location could be an important factor to be considered. The additional information such as range, energy and quality of the nodes could also be generated and assigned to a node along with the location information. Throughout this paper the novel agglomeration mechanism concentrates on the location of a node, and assumes the locations X, Y value are the keys used for security. If a node tries to cheat during communication, it is restricted from doing so and can be removed from the initial location. The planning and development of the routing protocol supported agglomeration is explained below.

The Network is assumed that N numbers of soldiers [Nodes] are elected in a Military zone considered as the network area and these soldiers are appointed from different categories like state. Based on the number of nodes, a constant k is defined to create the number of clusters [groups] in the network. The nodes clusters are formed by placing the nodes category wise in each cluster in a random location [x, y] within the cluster area and assigning the same [x, y] location as the key to that particular node. In the proposed approach clustering the nodes is done in such a way that each cluster can have at least one node selected from each category as depicted in figure-1a, b.

From the above figure it is clear that the 50 nodes are taken from 5 states where 10 from each state and these nodes are placed in 10 clusters (10 x 5 = 50). The nodes are placed in a location in clusters the nodes square measure set in [x, y] co-ordinate system, where the [x, y] values square
measure allotted because the key try to every node and it obtained by the Equation-[1]. For further communication, this key pairs should be submitted for permission and begin communication with each other. If any node without the key pair in the network and try for communication, it will be eliminated or rejected from the communication. In the real time the node information processing address (IP address) is blocked and again the node cannot get access into the particular network.

$$key(\text{node}_i) = \sum_{i=0}^{n} \text{node}_i(x_i, y_i)$$

(1)

**Algorithm:**

```
Algorithm:
1. Network G = \{N_1, N_2, \ldots, N_M\} \times \mathbb{R}, \ N \text{ is the number of Nodes in the network } G 
2. define K where K = \frac{P}{k}, k \text{ is a constant}
3. \text{for} i = 1 \text{ to } M
4. \text{for} t = 1 \text{ to } k
5. if(\text{key}(N_0) = N(x, y))
6. \text{end if}
7. \text{end for}
8. if(\text{isa}(N(x, y) = \text{key}(N_0)) then
9. \text{N1} = \text{message to BS}
10. \text{updateEnergy}(N_0)
11. \text{end if}
12. \text{Next}
13. \text{Next}
14. \text{for} t = 1 \text{ to } k
15. \text{if(\text{N1}(x, y) = \text{key}(N_0)) then
16. \text{N2} = \text{message to BS}
17. \text{updateEnergy}(N_1)
18. \text{end if}
19. \text{Next}
20. \text{Next}
21. \text{for} t = 1 \text{ to } k
22. \text{CH} = \text{max}(\text{min}(\text{energy}(N_0)))
23. \text{Next}
24. \text{for} t = 1 \text{ to } k
25. \text{CH} = \text{aggregateData}(\text{CH}, \text{data}_i, \text{N1})
26. \text{Next}
27. \text{for} t = 1 \text{ to } k
28. \text{BS} = \text{aggregateData}(\text{BS}, \text{data}_i, \text{N1})
29. \text{Next}
```

The network G contains the M range of nodes [N] and every node has its own characteristics like energy, base location and current location [x, y]. To save the energy, the proposed technique uses a new clustering method. It is assumed that the nodes are from completely different states and are to be placed in the Head Location of a country. The parameters like range, residual energy and the quality of nodes taken from each state. The range of clusters or the quantity of clusters in the network is the number of nodes taken from every state. It implies that every cluster ought to have at least one node from one state, all the remaining nodes in the cluster belong to all or any of the state. When a node is initialized or placed in a cluster at (x, y), these x and y value is assigned as the private key and public key respectively to that particular node. Once a node is initialized and clustered every node ought to send a hello message to the Base Station (BS) when their key pair is validated. According to the distance and message size, all the nodes loose some energy. Based on the energy value, the
highest energy node is elected as Cluster Head (CH) in each clusters, and the cluster nodes communicate to the base station with the help of the CH, where CH gather and aggregate the data to the BS. The CH election process is applied in the network in a particular time interval. Due this the energy is saved and the node is become a trustable nodes.

Simulation Settings

This proposed algorithm is coded in Network simulator 2 (NS2) and the performance of the proposed approach is verified. In the NS2, the size of the network is assumed as 1200 x 1200 and 50 number of nodes deployed in the network and clustered. There are 5 clusters where each cluster contains 10 nodes and each node belongs to one state, totally 10 states. The parameters of the nodes and the channel characteristics assigned in the TCL code are given in the following table.

Table 1: Simulation System parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X, Y</td>
<td>1200, 1200</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>PROB</td>
<td>Radio Propagation</td>
</tr>
<tr>
<td>NN</td>
<td>MAC/802.11</td>
</tr>
<tr>
<td>MAC</td>
<td>Energy-model=true</td>
</tr>
<tr>
<td>Mobility</td>
<td>Random</td>
</tr>
<tr>
<td>Moving Speed</td>
<td>2 m/s</td>
</tr>
<tr>
<td>Traffic</td>
<td>CBR</td>
</tr>
<tr>
<td>Bandwidth Link</td>
<td>2 Mbps</td>
</tr>
<tr>
<td>Propagation path loss model</td>
<td>Two-Ray ground Model</td>
</tr>
</tbody>
</table>

NS2 version 2-3.4 has been used to analyze the proposed approach with the routing protocol AODV. The under lying MAC protocol defined by IEEE 802.11 was used Traffic sources of both continuous bit rate (CBR) based on TCP for 10 sources were generated. The CBR and TCP mobility scenario of 20 nodes with a maximum speed of 30 seconds and for a simulation area of 1200 × 1200 with 2.0 Mbps was generated.

Simulation Results & Discussion:

The misbehavior of the malicious nodes in the network is incorporated in the same way as done in (M. Kaniganti, 2003). By taking the number of nodes in network as 25, 50, 75, 100 the proposed approach is implemented. The misbehaving node is detected only by verifying the key pair that is if and only if the node belongs to the particular cluster and in the particular network region, it is allowed to communicate. According to the simulations based on number of nodes, the result is generated and given in graphical form for analyzing the performance.

During simulation the important factors of the network namely energy, malicious node detection rate and the throughput are captured from the trace file and plotted as a graph. The following Figure-2 shows the number of malicious node detected in a given period for the proposed approach as well as the existing approach. The number of malicious node detected by the proposed approach is less than that in the existing approach since the malicious activity is reduced in the proposed approach during the initialization of the network itself. Even though few nodes try from outside the network to act as malicious; they can be detected accurately by the proposed approach. The detection rate is shown in the Figure-2 clearly. In context of energy saving, the proposed approach retains more energy than the existing approach and it is clearly depicted in Figure-4. The proposed approach retains 94.58%, 91%, 86% and 81.34% of the energy in all the four rounds with 25, 50, 75 and 100 nodes respectively where the existing system retains 91%, 84%, 77% and 73% of the energy in all the four rounds with 25, 50, 75 and 100 nodes respectively.

The packet success rate transmission can be obtained by reducing or eliminating the packet loss. This proposed approach gives best success packet transmission and it is clearly shown in Figure-3. Comparing with the existing approaches, the proposed approach obtained 4 to 10% of packet transmission rate more. In terms of throughput the proposed approach obtained more successful transmission than the existing approach and it clearly depicted in Figure-5. The proposed approach transmitted 43000, 54000, 65000 and 78900 packets in all the four rounds with 25, 50, 75 and 100 nodes respectively where the existing system transmitted 42500, 51345, 63749 and 71234 packets in all the four rounds with 25, 50, 75 and 100 nodes respectively.

Conclusion:

It is concluded that the proposed approach is better than the existing approach in terms of detection rate, energy minimization, throughput and packet transmission rate are clearly depicted in Figure-2, 3, 4 and 5. The clustering mechanism saves the energy at each node as well as in the network and increases the network life.
time. As the location key pair is assigned as the dynamic random key, it cannot be modified or duplicated by any one thereby provides high security to all the nodes in the network. Hence this proposed approach provides more reliable and better performance than the existing approaches.

**Fig. 2:** Detection Rate by Proposed System vs. Existing System.

**Fig. 3:** Packet Transmission Comparison.

**Fig. 4:** Energy Consumption by Proposed approach vs. Existing approach.

**Fig. 5:** Throughput obtained by proposed system vs. Existing System.

**REFERENCES**


