Base station augmentation using multipath in WSN

Deepika Tyagi[1] Mrs. Sarita Choudhary[2]
[1, 2] Deptt. Of CSE & Doon valley inst. of Engg. KUK

Abstract--- Wireless Sensor Networks (WSNs) are prepared of sensor nodes with constrained battery life and diffusion potential. Routing protocols in wireless sensor networks (WSN) have been considerably investigated by researches. Wireless sense network have various challenges in which there is one security. Security is major concern in wireless sense network to improve security we try to enhancement the base station security by providing multipath routing technique. Multipath routing technique overcomes the various problems of single path routing as integrity, authentication, availability-resilience-self healing, and confidentiality by providing various multipath ways for the data transmission.

Keywords: Wireless Sensor Networks, Sensor Nodes, Secure Routing, Protocols, Base Station.

I. INTRODUCTION

Wireless Sensor Networks are efficiently place low cost, low processing power, less memory and incline energy resource networks. In topical years WSN found an extraordinary amount of applications in the lawn of both research and academics. In WSN, the nodes are called sensors which sagacity the data like heat up, dampness, clamor or sound, pressure soil assortment, actions of objects, stress levels, recognition of objects approximately and other properties from the adjoining and send this information to the base station for further analysis and decision making. WSN are mainly place in predictable environment where the sensor nodes suffer desolate and used for inquiry and monitoring. WSN finds a large consequence in the fields evocative of armed, traffic supervise, home computerization, healthcare applications and many civilian application areas. Since WSN sensor nodes are place in desolate and bumpy natural environment there are phenomenal number of security issues with them. Data transmitted in WSN should be fortified from unauthenticated and unauthorized nodes and attackers. We have to maintain the legality, sincerity and discretion of the data that is transmitted between the nodes of the network. Fraud may attack the network in many civilization as jampering and overcapacity the data packets affect the reliability, unauthorized access to the network (Eavesdropping), confess to be legal node to lock up the data.

II. RELATED WORK

Wireless Sensor network security is a critical issue in sensor network research. Ganesan et al propose a redundant multipath routing approach for a sensor network [4] in order to provide fault tolerance and reliable data dissemination. Deng et al. [12] propose to use multipath in sensor network to tolerate intrusions to sensor network. Chan et al. [21] propose to use multipath for the two nodes communication in sensor network. We have proposed a routing scheme that uses multiple paths and multiple base stations to tolerate the attacks to sensor node and base station. Paper [10] dealt with the simulation of two wireless sensor network localization algorithms: the weighted centroid localization algorithm and the iterative trilateration. The algorithm was simulated using a fixed number of sensors and a variable number of anchors. Three anchor deployment scenarios were used. In order to obtain a clear picture of the algorithm results average error were calculated. After observing the average errors obtained for the uniform and random anchor placement using the WCL algorithm, an improvement solution for the random placement was obtained. This solution, called hybrid approach, leads to significant error reduction, especially when using a small number of anchor nodes. Therefore it can be concluded that by using the hybrid approach the error introduced by the random anchor placement is reduced. This makes the new approach a favorable one. Staddon et. al [9] propose a protocol for base station to get neighbourhood information of sensor nodes. This protocol doesn't consider the case of sensor node compromises. Deng et. al [12] use a secure network setup algorithm similar to our route discovery protocol, to find the network topology. Our routing protocol also differs from [12] in that it supports multiple base stations. [12] proposes multiple path routing to povide intrusion tolerance in sensor networks. However, [12] is based on single base station.

III. MULTIPATH ROUTING PROTOCOL

An imperative objective in constructing multiple outmoded routes is to diminish the harm a malicious node may impose. In finicky, a malevolent node has a superior opportunity of inflicting spoil on nearby nodes, for example by induction an attack. So, we prefer two sovereign paths in such a mode that the nodes in the two paths are far apart. For a sensor node A, this is done as follows. The first path from A to the nearby base station is elected using the breadth-first search shortest path algorithm. To conclude the second path, three sets of nodes, X_1, X_2, and X_3 are first constructed. X_1 is the set of nodes belonging to the first path, X_2 is the set of nodes belonging to X_1 and any neighbor nodes of the nodes in X_1, and X_3 is the set of nodes belonging X_2 and any neighbor nodes of the nodes in X_2. All three sets exclude a or the base station. The second path is then computed as follows.

1. Remove all nodes in X_3 from the network, and find the shortest path from A to a base station. If such a path is found, terminate the computation. The path found it is the second path.
2. Remove all nodes in X_2 from the original network. Find the shortest path from A to a base station. If such a path is found, terminate the computation. The path found it is the second path.
3. Remove all nodes in X_1 from the original network. Find the shortest path from A to a base station. If such a path is found, it is the second path. Otherwise, there is no second path from A to the base station.

A fascinating question is which base station should be elected for the second path? There are at least two diverse strategies possible here. In the first approach, the second path is select based on the method describe above, irrespective of which base position it leads to. In finicky, the second preventable path may lead to the equivalent base

station as the first path. In the second strategy, the second path is chosen based on the method describe above, but with a supplementary constriction that this corridor must lead to a diverse base station than the base station in the first path. If such a second path cannot be found, then we lapse back to the first approach. Thus, if the second tactic is used, some sensor nodes may have outmoded paths foremost to diverse bases stations, while others may have outmoded paths foremost to the same base station. Finally, depending on the network topology, it is undeniably doable that no second outmoded path is initiate for several sensor nodes. In that case, the recent execution maintains only a single path. After computing the disused paths and forwarding tables for each node, meticulous base stations proliferate these tables to the meticulous nodes in a breadth-first manner. A base station first sends the forwarding tables of all nodes that are its abrupt neighbors. It then sends the forwarding tables of nodes that are at a distance of two hops from it, and so on. This instrument shrewdly uses the outmoded routing apparatus just built to dole out the forwarding tables. Standard security techniques such as those proposed in can be used to distribute these forwarding tables in a secure manner.

IV. Simulated Results

Simulation Of The Approach In Done On Matlab. Here In Step By Step Presentation Of The Mutlipath Routing Approach Simulation On Matlab. In The Figure 2 It Shows Node Deployment Where The User Will Enter The Number Of Sensor Nodes To Be Deployed.

Fig. 1: Node deployment

In the simulation shown below (figure 3) after nodes are deployed now we select started node and destination node, the sender node will become starting Node and will send request for authentication to each node.

```
enter the starting node 4

n =

     4

enter the destination node 9

m =

     9
```

Fig. 2: Nodes defined

Various nodes creating various paths for the transmission of data or packets and also calculating the cost of the path which we will select for the transmission of data as shown figure 4 multipath ways.

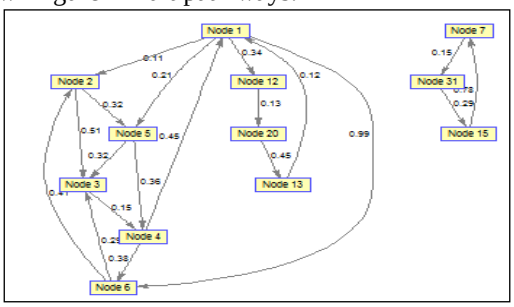

Fig. 4: multipath process

In this figure 5 the starting nodes and destination node selected by the user and the cost. The path is shown on which the data will transmitted through to the destination.

```
enter the starting node 4

n =

     4

enter the destination node 9

m =

     9


cost =

    15


path =

     4     7     9
```

Fig. 5: path selection

V. Conclusion

Security is one of the key concerns in Wireless Sensor Networks because of the network deployment. Impostor can assail the network in many ways, it could be physical or by gaining access to real node. A large amount of security mechanisms are purposed in Wireless Sensor Network out of which one is multipath routing technique. In the thesis enhanced the security of base station with adding multipath routing method. We simulated the environment in various situations that is network with mesh network, with single path, and with the multi-path . With the results we have seen that the cost, speed and the energy. Hence, it secures the network more than the existing single path technique.

References

[1] Culler, D.E and Hong, W., "Wireless Sensor Network", Communication of the ACM, Vol.47, No. 6, June 2004, pp.30-33.
[2] Akyildiz, I. F., Su , W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.
[3] Chonggun kim, Elmurod Talipov, and Byoungchul Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", International Federation for Information processing, 2006, pp. 522-531.
[4] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, "Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks," Mobile Computing and Communication Review (MC2R) Vol 1., No.2. 2002.
[5] Kemal Akkaya and Mohamed Younis, " A Survey on routing protocols for wireless sensor networks", Elsevier,2003.
[6] CHEE-YEE and SRIKANTA P. KUMAR, "Sensor Networks: Evolution, Opportunities, and challenges", Proceeding of the IEEE, Vol.91, No.8, Aug 2003.
[7] Jan Steffan, Ludger, Mariano Cilla, Alejandro Buchmann, "Scoping in Wireless Sensor Networks", ACM, 2004.

[8] Jyoti Shukla and Babli Kumari, "Security threats and Defense Approaches In Wireless Sensor Network: An Overview", IJAIEM, Vol. 2, Issue 3,Mar 2013
[9] M. Gholami n, N.Cai, R.W.Brennan "An artificial neural network approach to the problem of wireless sensors network localization" Robotics and Computer-Integrated Manufacturing 29 (2013) 96–109
[10] Rusnac, R.-I.; Gontean "Evaluation of wireless sensor networks localization algorithms" Volume: 2 Publication Year: 2011, Page(s): 857 - 862 Shio Kumar Singh, M P Singh, and D K Singh, " Routing Protocols in Wireless Sensor Networks- A Survey", IJCSES, Vol .1, No. 2, Nov 2010.
[11] Y. Hu, D. Johnson, A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02).
[12] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security issued in Wireless Sensor Networks", International journal Of Communications, Vol.2, Issue. 1,2008.
[13] Elmurod Talipov, Donxue Jin, Jaeyoun Jung, Ilkhyu Ha, YoungJun Choi, and Chonggun Kim, "Path Hopping Based Reverse AODV for Security", Springer, pp. 574-577, 2006.
[14] A. Agah, S. K. Das , K. Basu, and M. Asadi. "Intrusion detection in Sensor Networks: a Non- Coorperative Game Approach", IEEE, pp. 343-346,2004.
[15] C. Bekara and M. Laurent-Maknavicious. " A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks", IEEE, pp.59-59, 2007.
[16] C. Blundo, A.D.Santis, A. HerzBerg, S. Kutten, U. Vaccro, and M. Yung. " Perfectly- Secure Key distribution For dynamic Confrences", Information and Computation, pp. 1-23, 1998.
[17] R. Brooks, P.Y. Govindaraju, M.Pireretti, N. Vijaykrishnan, and M. T. Kandemir, " On the Detection Of Clones in Sensor Networks Using Random Key Predistribution, IEEE,pp. 1246-1258,2007.

