Preventive Alternate Path Routing Algorithm against Intrusion in Sensor Area Network

Swimpy Pahuja and Anita Singhrova

***Abstract*—This paper presents a secure alternate path routing scheme in the field of wireless sensor networks. Our alternate path scheme provides a non-greedy route establishment approach for data dissemination among spatially distributed sensor nodes in wireless sensor networks. It proposes the new algorithm for the purpose of path computation which starts from the initialization of the network. The algorithm has been designed to improve routing security in wireless sensor network. The algorithm uses alternative routing paths for each data transmission call to overcome the sensor network attack. To enhance network reliability, the algorithm allows sensory data to be sent on defined routing paths using various intermediate transmission nodes.**

***Index Terms*—Alternate path, intrusion avoidance, sensor network, shortest path.**

I. Introduction

Wireless Sensor networks (WSN) can be defined as the network of self-organizing, resource-constrained tiny sensor nodes capable of sensing physical as well as environmental conditions. These tiny sensor nodes communicate with each other using low power wireless data routing protocols [1]. As the exact location of sensor nodes cannot be predetermined, they can be deployed randomly inside inaccessible areas without any human intervention. Hence, WSNs are fault tolerant and have self-organizing capabilities. The sensor nodes have limited power, memory as well as computing elements which motivates the researchers to develop proper mechanisms for efficient utilization of these highly resource-constrained nodes in sensor area networks.

Wireless sensor network acts as a bridge between real world and computation world as shown in Fig. 1. Wireless sensor networks are subclass of ad hoc network wherein group of sensors capable of making measurements exchange data packets among them.

It consists of a base station or gateway that can communicate with a no. of wireless sensors via a radio link as shown in Fig. 2.

Manuscript received September 2, 2012; revised November 17, 2012. This work was supported in part by the Deenbandhu Chhotu Ram University of Science and Technology (DCRUST), Murthal.

S. Pahuja is with the M. Tech. in CSE from Deenbandhu Chhotu Ram University of Science and Technology (DCRUST), Murthal. She is now with the HOD of CSE Department in Rayat Bahra Innovative Institute of Technology and Management (RBIITM) (e-mail: swimpy.pahuja@gmail.com).

A. Singhrova is with the CSE Department in Deenbandhu Chhotu Ram University of Science and Technology (DCRUST), Murthal (e-mail: nidhianita@gmail.com).

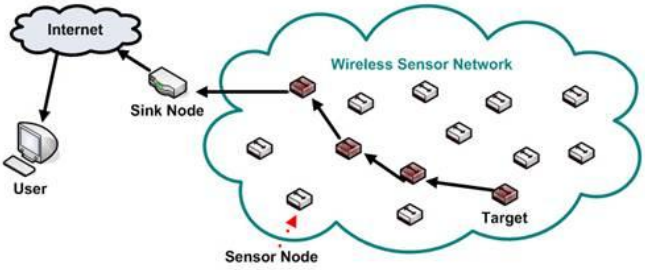

Fig. 1. Wireless sensor network as a bridge [1].

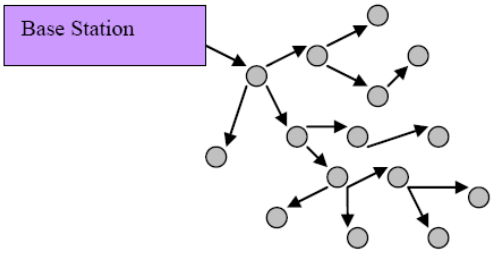

Fig. 2. Wireless sensor network.

Data is collected at these sensor nodes where it is compressed and transmitted to the gateway directly or via other intermediate sensor nodes.

A. Need for Security in Sensor Networks

In the near future, WSN will play an essential role in various real life applications. Security is a great challenge in these networks due to enormous reasons. Deployment of sensor nodes in non-monitoring and unreachable environments makes individual sensors vulnerable to security compromise and susceptible to physical capture. Sensor nodes are resource constrained in terms of memory, power and computation resources, and using wireless link for sensor nodes communication, further increase nodes susceptibility to common attacks against wireless network [2].

Many routing and data transfer protocols have been specifically designed for WSNs [3], [1] but only some of them have been designed with security as a necessity. Most sensor network routing protocols are, however, quite simple and for this reason are sometimes insecure. In what follow, we present a discussion of major attacks against them.

B. Attacks on Sensor Networks

Various types of network layer attacks against sensor networks are as follows [4].

1) *Sinkhole attacks:* to make the compromised node look attractive to surrounding nodes with respect to the routing choice.
2) *Spoofed, altered routing attack:* to replay routing

information, create routing loops, and to extend or shorten source routes.

3) *HELLO flood attacks:* broadcast HELLO packets to announce themselves to their neighbors and define new node.
4) *Sybil attacks:* a single node presents multiple identities to other nodes in the network.
5) *Wormholes:* adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part.
6) *Selective forwarding:* refuse to forward certain messages, to simply drop them, and to attract or repel network traffic.
7) *Acknowledgement spoofing:* spoof link layer acknowledgments for "overheard packets" addressed to neighboring nodes.

Therefore, we are providing an approach to prevent our confidential information from intruder attack by proposing an alternate path scheme.

II. Existing Routing Scheme

A. Shortest Path Scheme

Various data routing schemes computing shortest route to destination node for data packet distribution have been reviewed in the literature. Some of them includes Dijkstra's algorithm [5] which solves the single-pair, single-source, and single-destination shortest path problems, Bellman-Ford algorithm [6] which solves the single source problem where edge weights are given negative values, Floyd-Warshall algorithm [7] which solves all pairs shortest paths etc. But secure data transmission is not the main goal for all of them.

As the eavesdropper follows greedy approach such as Dijkstra's algorithm for stealing the confidential information, let us put some light on Dijkstra's algorithm.

The solution to shortest path computation problem was given by Dijkstra's algorithm which is a graph search algorithm that solves the single-source shortest path problem for a graph having positive edge weights, producing a shortest path tree. This algorithm is mostly used by various sensor nodes for the purpose of routing data packets over wireless sensor networks. For a given source vertex (node) in the graph, the algorithm finds the path with lowest cost (i.e. the shortest path) between that vertex and every other vertex as shown in Fig. 3. It can also be used for finding costs of shortest paths from a single vertex to a single destination vertex by stopping the algorithm once the shortest path to the destination vertex has been determined.

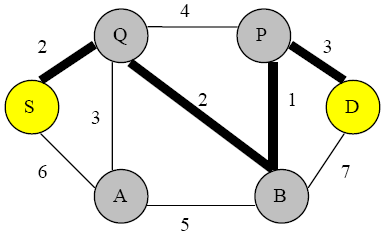

Fig. 3. Shortest path graph problem.

In the above Fig, 'S' denotes the source node and 'D' denotes destination node. Dark lines denote the shortest path obtained by applying Dijkstra's algorithm.

B. Alternate Path Scheme

Large number of algorithms for alternative route computation has been designed till now but their main objective did not revolve around secure transmission. Much of the research work carried out in the literature has focused on load balancing or effective utilization of highly resource-constrained sensor nodes.

Marta M.B. Pascoal, M. Eugenia V. Captivo and Joao C.N. Climaco [8] presented an algorithm for ranking loopless paths in undirected networks.

Villeneuve and G. Desaulniers [9] designed an algorithm for shortest path problem along with forbidden paths. It involves use of two algorithms namely k-shortest path problem and keyword matching algorithm to compute the desired path. Daniel Zappala [10] proposed a receiver-oriented alternate path protocol which is a local search heuristic that allows receivers to find alternate paths using only partial network information. This protocol is specifically designed for the purpose of load balancing.

Although some research has been carried out for secure protocol design also. Deng et al. [11] have designed an intrusion-tolerant routing protocol for sensor networks called INSENS which sends every data packet along multiple independent paths but requires feedback message to be send by each node to base station during route discovery phase introducing extra amount of overhead. S.B. Lee and Y.H. Choi [12] provided an alternate path approach which is resilient in the presence of several compromised nodes launching selective forwarding attacks. It uses neighbor report system for the detection of malicious node. Although it provides prevention as well as detection but it is more complex. Thus, we provide a simple and efficient preventive approach for avoiding unsafe route to destination.

III. Proposed Plan

Network layer applications are more prone to intruder attacks as wireless link is utilized for communication purpose among various types of networks. So, intrusion is one of the common problems in all networks; sensor networks face the same problem. Since sensor networks are densely deployed, transmission of confidential data over such networks demands high degree of security. But in case of man in middle attack, it is never easy to say a network is intruder safe. Even if the intruder knows about the routing algorithms or the algorithm implementation, it is quite difficult for him to handle the problem. One of such algorithm is generally followed by a user over the network is the shortest path computation algorithm. When intruder want to hack some information by acting man in middle, it is not easy for him to trace all the densely deployed nodes over the network. In such a case instead of tracking each node, intruder follows a route or the pattern to perform the attack. One of such method is to trace the shortest path. Generally, each routing algorithm follows the concept of shortest path as shown in Fig. 4 to transfer the data over the network with minimum delay as

well as cost requirements.

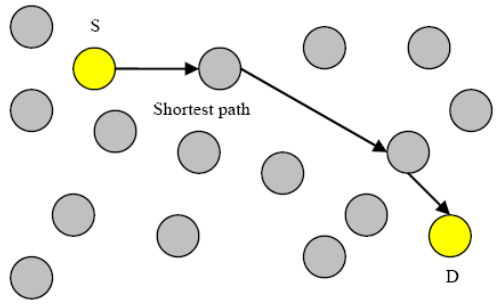

Fig. 4. Shortest path route nodes.

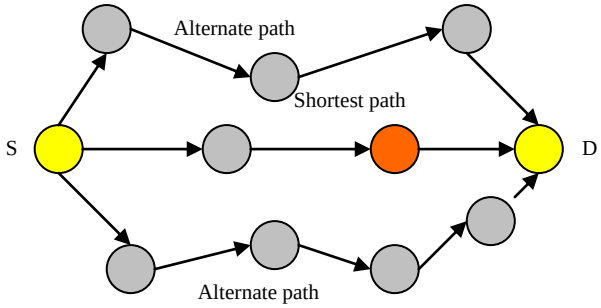

Fig. 5. Data routing using alternate path scheme.

In other words, we can say shortest path route nodes are the most unsafe nodes for transferring data as they are generally targeted by the intruder. An intruder tracks these shortest path nodes by attacking them from outside or by compromising a shortest path route node. The solution to such attacks is provided by finding an alternative route to the destination node and by getting the proper acknowledgement from the destination node.

The attack-prone wireless link and the dynamically changing topology signify that the wireless sensor networks require an optimized security oriented approach for designing routing protocols.

The attack possible is man in middle attack. The possible solution is given to the attack which uses the alternative route finding algorithm. The technique uses the method to find the alternative route as shown in Fig. 5 which is not the shortest one. So, our proposed plan is to select the alternate route in a network by avoiding compromised nodes in route selection process.

Their advantage is that the intruder may not be able to attack on the routing information as he would not be aware of this new route and the confidential information would reach its designated node without any eavesdropping and alteration. This would mainly be required in military applications as well as safety-critical applications.

Although there are huge amount of sensor nodes in sensor area networks but for the sake of simplicity few of them have been shown.

IV. Algorithm for Finding Alternate Path

The network establishment takes place from the starting i.e. initially all the nodes are in power off mode. This enables the sensor nodes to save their energy resource. Thus, the network defines sensor nodes to exist in various modes such as:

- Power off mode
- Ready mode
- Wait mode
- Processed mode

Power off mode indicates that the particular node is in energy-saving state; Ready mode signifies that nodes are ready to be processed; Wait mode states that nodes are waiting to be processed and processed mode indicates that nodes have been processed to compute the desired path. The algorithm uses two data structures stack as well as priority queue. The queue contains nodes in wait mode while the stack contains nodes in processed mode.

The proposed System is divided into four phases:

- Sensor nodes initialization phase
- Selection and scheduling phase
- Processing phase
- Alternate path computation phase

In first phase, network topology is created in which all the sensor nodes are in power off mode in order to save some amount of energy. This mode is then changed to ready mode i.e. nodes are ready to be processed or ready to route the sensory data over the sensor area network.

Now in next phase, if a node desires to route data packets then it is selected and kept into priority queue (now the node is in wait mode).

In the processing phase, we would remove the first node present in the priority queue and put it into the stack after adding all its neighbors to rear end of the priority queue. Duplication of nodes in priority queue is not permitted. This process continues until the queue becomes empty or the destination is reached.

The last phase i.e. path computation phase forces the algorithm to stop if the destination is reached and the alternate route is determined by removing the nodes from the stack.

Alternate Path Computation

- Set *P*_off =1
- if *P*_off =0

then put source node *M* in queue

- if node is already in queue

then do not add it again
else
{
for (*q*=1; front = rear = 0,
front = rear = destination node; *q*++)
{
for(*s*=10; *s*<1; *s*--)
{
Stack[*s*] = queue[*q*]
front = front + 1
Put all adjacent nodes of node M at
the rear end of queue
rear = rear + 1
}
}
}

- Return computed path by removing the nodes from stack.

A. Algorithm

The algorithm defines a binary variable *P*_off denoting the power save mode of sensing devices. If the value of this variable is set to 1, then it is said to be in power off mode or we can say, energy-saving mode. Otherwise, node would be in ready mode. '*q*' and 's' are the variables which keep track

of the location of respective node in the arrays of queue as well as stack respectively.

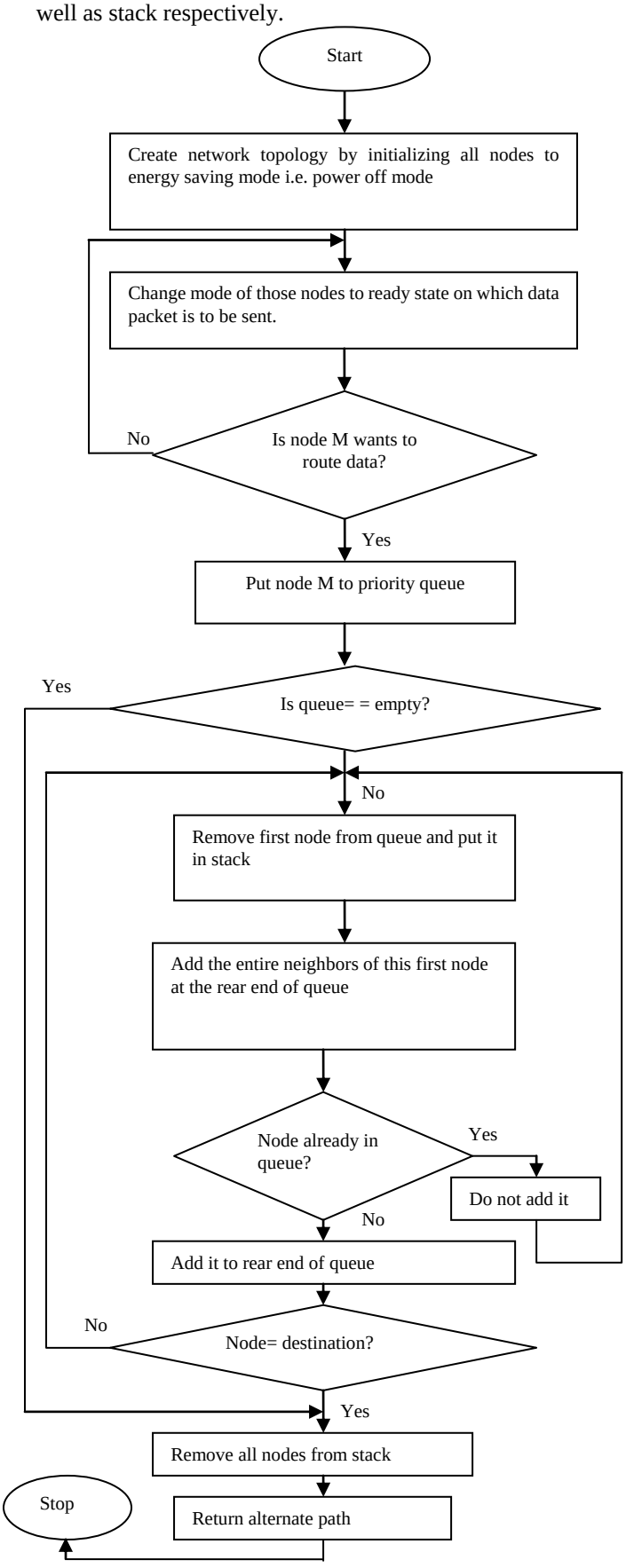

Fig. 6. Algorithmic flowchart.

B. Algorithmic Flowchart

The block diagram representation of given algorithm by means of flowchart is shown as under.

V. Conclusion

The shortest path is used to transmit sensory data over the sensor networks. The existing algorithm for finding this shortest path was given by Dijkstra which is not intruder safe and easily fall prey to intruder attack. In this paper, we have proposed an algorithm to determine alternate route to destination node without duplicating a particular node. Since nodes are not duplicated and exist in power off mode, the route computed is energy efficient as well as secure. Thus, network lifetime is also increased upto some extent.

As the shortest path is more prone to intruder attack, an alternate path which is secure from intruder attack has been proposed because intruder would be interested in shortest path; it won't be having any information about its existence.

References

[1] Q. F. Jiang and D. Manivannan, "Routing protocols for sensor networks", in *Proc. of the IEEE Conference*, pp. 93-98, 2004.
[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *University of California at Berkeley*, Tech. Rep. F33615-01-C-1895.
[3] N. N. Pham, J. Youn, and C. Won, "A comparison of wireless sensor network routing protocols on an experimental testbed," in *Proc. of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, 2006.
[4] B. Yang, "Study on security of wireless sensor network based on zigbee standard," in *Proc. of the International Conference on Computational Intelligence and Security*, pp.426-430, 2009.
[5] E. Dijkstra, "A note on two problems in connection with graphs," *Numerical Mathematics*, vol. 1, pp. 269-271, 1959.
[6] T. Korkmaz, M. Krunz, and S. Tragoudas, "An efficient algorithm for finding a path subject to two additive constraints," in *Proceedings of the ACM SIGMETRICS '00 Conference*, vol. 1, pp. 318-327, June 2000.
[7] C. E. Leiserson, *Introduction to Algorithms*, Second Edition, Chapter-24, pp. 630-635.
[8] M. M. B. Pascoal, M. Eugenia, V. Captivo, and J. C. N. Clomaco, "An algorithm for ranking quickest simple paths," *Computers and Operations Research*, vol. 32, pp. 509-520, 2005.
[9] D.Villeneuve and G. Desaulniers, "The shortest path problem with forbidden paths," *European Journal of Operational Research*, vol. 165, pp. 97-107, 2005.
[10] D. Zappala, "Alternate path routing for multicast," in *Proc. of the IEEE INFOCOM, Conference on Computer Communications*, pp. 1-10, March 2000.
[11] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing in WSN," in *Proc. of the Second International Workshop on Information Processing in Sensor Networks (IPSN 03)*, pp. 349-364, April 2003.
[12] S. B. Lee and Y. H. Choi, "A secure alternate path routing in sensor networks," in *Proc. of the Computer Communication*, vol. 30, pp. 153-165, 2006.

Swimpy Pahuja is M. Tech. in CSE from Deenbandhu Chhotu Ram University of Science and Technology, Murthal. She has done her bachelor's degree from Hindu College of Engineering affiliated to Maharashi Dayanand University, Rohtak. Presently, she is working as an HOD of CSE Department in Rayat Bahra Innovative Institute of Technology and Management (RBIITM), Sonepat and has an experience of serving Delhi Institute of Technology and Management for the full one semester. Her area of interest includes wireless sensor networks, ad hoc networks, RFID protocols etc.