International Journal of Science Engineering and Advance Technology

Seculation Routing With Fortification Wireless Networks

[1]Tikka Pallam Raju,[2] B S N Murthy
[1]Research scholar(M.Tech),[2]Associate Professor
Department Of CSE, Bonam Venkata Chalamayya Engineering College, Odalarevu,AP,INDIA

Abstract:
Wireless sensor networks having so many problems a number of solutios enough? security issues, discusses some existing solutions, and suggests possible research directions like key establishment secrecy,authentication,privacy,denial-of-service attacks ,secure routing and node capture attacks. Sensor devices are limited in their energy, computation, and communication capabilities Sensor nodes are often deployed in open areas, thus allowing physical attack Sensor networks closely interact with their physical environments and with people, posing new security problems. So In this paper address all the problems of wireless senor networks .In this paper we control back bone flooding attacks and give the location privacy These techniques provide trade-offs between privacy, communication cost, and latency.Through analysis and simulation, we demonstrate that the proposed techniques are efficient and effective for source and sink location privacy in sensor networks.

Keywords: Sensor networks, location privacy, dos, secure routing.

I Introduction:
In recent survey shows that than 80 internet operations demonstrated that non secure routing mechanisims these are not provide location privacy. The sporadic connection are established in these type of networks. A wireless sensor network (WSN) typically consists of a large number of small, multifunctional, and resource constrained sensors that are self-organized as an ad hoc network to monitor the physical world. Sensor networks are often used in applications where it is difficult or infeasible to set up wired networks. Examples include wildlife habitat monitoring, security and military surveillance, and target tracking. For applications like military surveillance, adversaries have strong incentives to eavesdrop on network traffic to obtain valuable intelligence, Providing location privacy in a sensor network is challenging. First, an adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. During non attack periods, routers are required to observe and routed entropy variations. Once the attackers is launched the entropy rate increases dynamically to identify the locations of zombies. Upstream routers helps to identify where the attack flow cause from based on their local entropy variations that are mentioned.

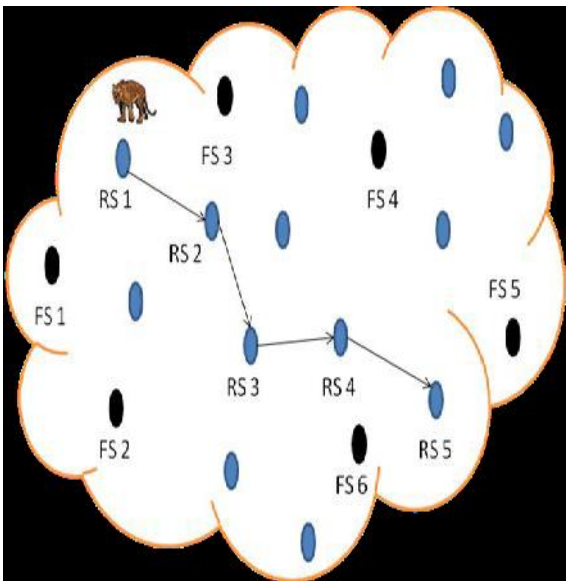
II Problem Statement:
Providing source nd sink privacies are most difficult tasks in WSNs. To begin with, an attacker is present in the same wireless medium as that of the defender and with no trouble the attacker can analyze the traffic pattern and intercept the network traffic. He can use the analyzed information to launch active attacks such as node compromising, data modification or data injection. Subsequently, sensors that are deployed are having limited processing speed and energy supplies. The existing system uses the approach of network coding which is carried out in three steps i.e. source encoding, intermediate recoding and sink decoding[6]. In source encoding step the messages belonging to same generation are encoded with the tag and are transmitted to the next hop. Every intermediate sensor nodes that is present between the source and destination perform the process of intermediate recoding. After obtaining the required number of messages from the previous node, random combination of the messages is formed and then forwarded to the next node. This process is repeated until the messages reach the destination.In these type of networks attacks are entrred in this way

1) Attacker first establishes a network which is responsible for huge volume of traffic to deny the series of normal users.
2) Attackers then discover vulnerable hosts of the network. Vulnerable host in the sense that the system running no anti viruses or out of date anti viruses software.
3) Attackers The now install new programs known as attack tools on the compromised hosts.
4) It can be shown by the growth of entropy rate from the point of attack.

III Proposed Work:

We propose three algorithms to increase the security and reduce the energy consumption of the sensor nodes' battery, (1) Finding the coverage set of sensors that can transmit at same time using Source Simulation method; (2) We propose an algorithm to compute the shortest path between source and destination and (3) We follow the principle of network coding on the messages that will traverse the network. The architectural design for the proposed system is shown in the figure 3 below:- Fig 3: - System architecture of the Privacy Protection against Global Eavesdropper using Network Coding Viewer is the front end of the system. User configures the system as well as the view to observe the output results using the viewer. User will configure the number of nodes to be present in simulation and the data sending time for the nodes. Using the wireless channel medium nodes communicate with each other and as well as with the sinks. Attacker will listen for all messages on wireless channel and try to identify the source location of packet. Sink use the coverage set finder to identify the set of nodes belonging in one set and using algorithm we propose the optimal path from node to the sink is calculated. Network coding mechanism is implemented in all the nodes present in the network so that privacy of each packet traversing the network is achieved. After sink receives the packet from the nodes, it uses network decoding/source decoding method to obtain the real message. Viewer Node Sink Coverage Set Finder Find set Initialize set Wireless Channel Attacker Data sending time Network Coding Network Decoding. One benefit of a wireless sensor network is the fine-grain sensing that large and dense sets of nodes can provide The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station Depending on the architecture of the network, aggregation may take place in many places All aggregation locations must be secured If the application tolerates approximate answers, powerful techniques are available Randomly sampling a small fraction of nodes and checking that they have behaved properly supports detection of many different types of attacks.

To reduce the energy consumption in WSNs we prefer to reduce the total number of potential sources in the network [7]. We create multiple candidate traces in the WSN in order to conceal the traffic generated by the real sources. The application in the system determines the number of candidate traces to be generated.



In source imitation method, set of fake sources are created in the network field. As shown in figure 3, many sensor nodes are deployed in the field where RS is Real Source and FS is Fake Source. When an event is reported at RS1, the fake sources present in the network generates traffic pattern similar to that of the real source to confuse the attacker. Source imitation works as follows: Before deploying the sensor, we arbitrarily select a set of N sensor nodes and preload each of the randomly selected nodes with a token, each having unique ID. To analyze the behaviour of the real source, these tokens are circulated among different sensor nodes.

IV Future Scope

There are a number of directions that worth studying in the future. First, in this paper, we assume that the global eavesdropper does not compromise sensor nodes; he only performs traffic analysis without looking at contents of packets. However, in practice, the global eavesdropper may be able to compromise a subset of the sensor nodes in the field and perform traffic analysis with additional knowledge from insiders. This presents interesting challenges to our methods. Second, some applications may require both source and sink location privacy. It will be interesting to investigate issues arising from integrating the source and sink location privacy techniques. Third, while we believe that it is possible for a well-funded and technically-savvy adversary to obtain a complete picture of network traffic, we recognize that complete coverage and perfect traffic analysis may be beyond the reach of some attackers. It is thus very interesting to study location privacy issues when the adversary can see only a fraction of the network traffic and must deal with the complexities of wireless signals. Finally, it takes time for the

observations made by the adversarial network to reach the adversary for analysis and reaction. Studying the impact of such "delayed" analysis and reaction will be another interesting research direction.

IV Conclusion:

In this paper, we have proposed as efficient source imitation approach with the combination of network coding for preserving the location privacy in sensor networks. With the use of Homomorphic Encryption on Encoding Vectors, the proposed idea offers protection against traffic analysis attacks and also preserves the confidentiality of the messages. Because of the shortest path calculation, the data travels faster between sensor nodes and no computation is carried out in the intermediate nodes maintaining the energy reserve of the sensor nodes. The simulation evaluation demonstrates that the communication cost is increased with requirement of location privacy and becomes stable after reaching certain number of bits. In our future work we can further increase the location privacy by sink imitation approach to protect the location of destination node.

References

[1] M.Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks,". [2] Wensheng Zhang · Guohong Cao · Tom La Porta." Dynamic proxy tree-based data dissemination schemes for wireless sensor networks" May 2006

[3] http://en.wikipedia.org/wiki/Onion_routing.

[4] M. Rennhard and B. Plattner, "Introducing MorphMix: peer-to-peer based anonymous Internet usage with collusion detection," in *Proc. ACM Workshop on Privacy in the Electronic Society*, pp. 91-102, 2002.

[5] Sumit Jaiswal , Jaydeep Howlader, Prasenjit Choudhury" A Review Of Anonymous Communications– Mix. [6] Yanfei Fan, Yixin Jiang, Haojin Zhu, Jiming Chen, Xuemin Shen, *"Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks,"* IEEE Transaction on Wireless Communication, Vol. 10, no. 3, 2011

[7] Kiran Mehta, Donggang Liu, Matthew Wright, *"Protecting Location Privacy in Sensor Networks against a Global Eavesdropper"* IEEE Transactions on Mobile Computing, Vol. 11, No.2, 2012.