International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Catching Moles and Packet Droppers in Wireless Sensors Network

Mohammed Hajee[1], Mohammed Abdul Rawoof[2]

Nawab Shah College of Engineering & Technology (Affiliated to JNTUH), Hyderabad, Telangana, India

Abstract: ***While many protocols for sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. Existing techniques defend the leakage of location information from a limited adversary who can only observe network traffic in a small region. However, a stronger adversary, the global eavesdropper, is realistic and can defeat these existing techniques. This paper first formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead needed for achieving a given level of location privacy. The paper then proposes two techniques to provide location privacy to monitored objects (source location privacy) – periodic collection and source simulation – and two techniques to provide location privacy to data sinks (sink location privacy) – sink simulation and backbone flooding. 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 Network, Sink simulation, Backbone Flooding, Latency, cost.

1. Introduction

Wireless sensor networks (WSNs) have been widely employed in many diverse applications because of their ease of installation, cost efficient and portability. A wireless sensor network mainly consists of one or more sensing devices such as acoustic microphones video or still cameras, seismic or magnetic sensors. Each sensor node communicates wirelessly with a few other local nodes within its radio communication range. Even though wireless sensor networks are having these advantages, there are many drawbacks associated with them such as, weak system reliability, shorter coverage range and the most critical drawback is its privacy and security issues. One of the ways to increase the reliability and range of the WSNs is to employ multi-hop routing. The concept of multi-hop routing is to forward a packet to the destination using different path in case of the node failure. But, the critical issue still remains of providing security and privacy in WSNs. Therefore, preserving the privacy of the location of the source node remains critical. Wireless sensor networks are used in many areas such as military supervision where possibility of the eavesdropping the traffic is high to get hold of sensitive information. Exploitation of such information can cause economic losses or cause danger to human lives. To protect such information, researchers are finding out new ways to provide standard security services such as, availability, integrity, confidentiality and authentication. The exchange of information between sensors can disclose sensitive information which can reveal the location information of the critical modules present in the network the sensor networks are deployed to monitor the endangered animals in a forest. An event is triggered. whenever an animal is spotted in the monitored area. The hunter tries to gather this information and may capture or kill the endangered animal [1]. The above scenario depicts the vulnerability of WSNs is more because of its open wireless medium to transmit the information from source to destination. It is very challenging to effectively put a stop to these kinds of traffic analysis attacks and provide location privacy in WSNs. Existing schemes such as proxy-based schemes [2], onion routing schemes [3] and Chaum's mix-based schemes [4] [5], may moreover require a series of trusted proxies which can forward the data resulting in the degradation of the performance. These schemes are only capable of dealing with only local eavesdropper and to the limited section of the network. The deployment of network coding in wireless sensor networks can result in the high performance gain and also offer sufficient way to stop traffic analysis and flow tracing attacks. Similar to Chaum's mix-based schemes [4],[5], network coding provides built-in coding/mixing mechanism, which implies that privacy preservation is achieved in distributed manner. There is unlinkability between the both incoming and outgoing packets, which is a very important property for averting the traffic analysis attacks. In this paper which is based on network coding, we use Homomorphic Encryption (HE) on the Encoding Vector to achieve the efficient privacy in WSNs. With the use of HEs the confidentiality of the Encoding Vector is effectively guaranteed making it almost complicated for an adversary to obtain the plaintext. Instead of Link-to-Link encryption, End-to-End encryption on Encoding Vector is employed to achieve even energy efficiency and avoiding intermediate coding/mixing operations. In this paper we focus on the secure communication methods that preserve the privacy against both global and local eavesdropper. The contributions in this paper are threefold.

- We point out that the assumption of a global eavesdropper who can visualize the entire network and can monitor the traffic traversing the network. We apply the network coding mechanism by tagging the packets with the Encoding Vector.
- We apply the source imitation approach to find out the number of candidate traces present in the network and evaluate the proposed techniques for location privacy in sensor networks.

- We compute the optimal path between the source and destination to maintain the energy reserve in the sensor network

2. Literature Survey

Sensor networks feature two privacy concerns, data-oriented and context-oriented privacy. Data-oriented privacy deals with securing the integrity of data gathered and transmitted to the destination. Context-oriented privacy prevents adversaries form gaining access to data context information, such as the time and location from which, the data originated. Data-oriented privacy focuses on proving protection to data items. Attackers can corrupt or eavesdrop on data to obtain critical information or inject false information in the network. A passive adversary eavesdrops on communication between nodes to determine the location of nodes or tracks the evolution of events. Cryptographic schemes can mitigate this type of unlawful behavior. Active malicious nodes can inject polluted information into the network through these nodes. The main focus of context-oriented privacy is to ensure the privacy of context related information, such as the location and time. The location can refer to the node location or data origin location. If an adversary can detect the location of a sink or the area, where an event has occurred, it can breach the privacy of information. It may also track or compromise a sensitive critical target.

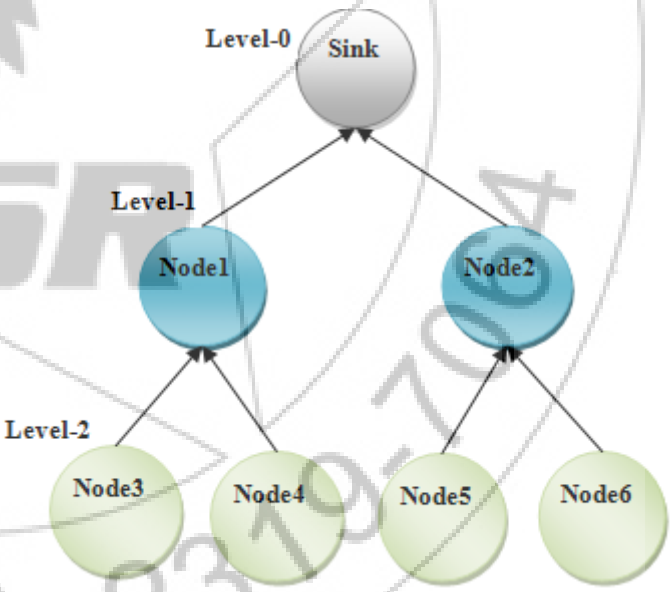
The problem of privacy preservation is addressed by perturbing the parameters that are monitored. The underlying probability distributions are changed such that definite patterns cannot be constructed from the perturbed data and the relationships between different entities are uncorrelated. Increasing the entropy also increases privacy (Mehta et al., 2007) by enhancing the crowd size or the diversity. This enhancement can be achieved by employing cryptographic or non-cryptographic mechanisms. Various non-cryptographic mechanisms have been studied in the literature. Random walk has been used in Phantom routing ,and randomized routing has been used along with flooding to hide the location of the source. Fake message injection and path perturbation algorithms are also used to randomize traffic patterns and reduce the probability of tracking mobile targets. The data are aggregated, or their coarseness is increased. Techniques to increase coarseness associated with location details have also been proposed. Cryptographic techniques for privacy complement non-cryptographic techniques, such as routing, virtual ring creation, etc. The choice of cryptographic technique is important, as it consumes resources of the network. This consumption may adversely affect the latency, throughput and network lifetime. Many approaches provide the privacy of nodes and data; while ensuring efficient resource consumption. A new time efficient source privacy scheme, TESP2, against the traffic analysis attack of a global eavesdropper that can monitor and analyze the traffic in the entire network has been proposed (Chen et al., 2012). In TESP2, a sensor node broadcasts a request for timed data collection to its upstream nodes. Each upstream node sends the cipher text of the real data or else sends the cipher text of the dummy data if it lacks any real data. To preserve the source privacy, the sensor node will discard any dummy data, re-encrypt and forward the cipher text of the real data to the downstream nodes.

3. Problem Definition

In this paper, we propose a simple effective scheme to catch both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established. When sensor data are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet.

The sink can figure out the dropping ratio associated with every sensor node, and then runs our proposed **node categorization algorithm** to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers.Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs our proposed node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers.As the information of node behaviors has been accumulated, the sink periodically runs our proposed **heuristic ranking algorithms** to identify most likely bad nodes from suspiciously bad nodes. This way, most of the bad nodes can be gradually identified with small false positive.

4. System Architecture



5. Methodologies

1) Node Configuration

- Link Configuration
- In this module Nodes are configured based on number of nodes in group. We create the network group by connecting nodes to sink. Link configuration means connecting the nodes and intermediate nodes to the sink.

2) Sender Node

- Packet Splitting

In this module, Sender selects the file which is to be sent. And then it split into the number of packets based on the size for adding some bits in it.

- Send Packets to Intermediate
  And then it encrypts all the splitted packets. And then sender adds some bits to each encrypted packets before sending that. Bit Addition for each packet is identification for sender. After adding of bits to each packet, it sends the packets to the nearest node or intermediate node.

3) **Intermediate Node**

- Send Packets to Sink
  In this module, the intermediate node receives Packets from the sender. After receiving all packets from sender, it encrypts all packets again for authentication. Before sending to sink, intermediate add some bits to each packet for node identification. After adding some bits from intermediate, it sends all packets to the sink.
- Modify or Drop
  Before sending all packets to sink, packets dropping or packets modifying may be occur in intermediate.

4) Sink

- Verify
  In this module, Sink receives all packets from the sender node, and it verifies all packets which are dropped or not. And it also verifies the packets which are modified or not and it can identify the modifiers in the process based on the bit identification.
- Merge Packet
  After receiving all packets in sink, it decrypts all packets. After the decryption if there is no modified or dropped packets, it merge all packets. After merging, Sink can receive the original file.
- Categorization And Ranking
  In this module Categorization and Ranking will be performed based on the node behavior. If there is any modification or drop of packets in node it assumes negative value for modifier or dropper. Sink performs Ranking for each node based on the Category of nodes. Sink gives ranking like Good, Temporarily Good, Suspiciously Bad, Bad based on the node behavior in the process

6. Conclusion and Future Work

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,” Proc. IEEE INFOCOM’08, pp. 51-55, 2008.
[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, 2013

Author Profile

Mohammed Hajee, working in Nawab Shah College of Engineering & Technology as an assistant professor in CSIT dept.

Mohammed Abdul Rawoof, working in Nawab Shah College of Engineering & Technology as an assistant professor in CSIT department