Volume : 2 | Issue : 11 | Nov 2013 • ISSN No 2277 - 8160

Research Paper Engineering

Preserving Communication System Using Detection and Localizing Multiple Adversaries in WSN

Balamurugan. D Asst. Prof CSE, Annapoorana Engineering College,Salem

A. Deepa Lecture, Annapoorana Engineering College,Salem

ABSTRACT

Wireless sensor network often support sensitive applications. These applications may require that users' identity, location, and correspondents be kept secret. This is a challenge in a WSN because of the cooperative nature of the network and broadcast nature of the communication media. In this paper, we propose a privacy preserving communication system (PPCS) which provides a comprehensive solution to anonymize communication end- points, keep the location and identifier of a node unlinkable, and mask the existence of communication flows. There are a number of directions that worth studying in the future. In particular, in this paper, we assume that the global eavesdropper will not compromise sensor nodes; he only performs traffic analysis without looking at the content of the packet. However, in practice, the global eavesdropper may be able to compromise a few sensor nodes in the field and perform traffic analysis with additional knowledge from insiders. This presents interesting challenges for both of our approaches. In addition, we are also interested in the implementation of our methods in real sensor platforms and the experimental results from real sensor applications.

KEYWORDS : Sensor networks, location privacy

Introduction:

In recent years, wireless sensor networks (WSNs) have drawn considerable attention from the research community on issues ranging from theoretical research to practical applications. Special characteristics of WSNs, such as resource constraints on energy and computational power, have been well defined and widely studied [3]. What has received less attention, however, is the critical privacy concern on information being collected, transmitted, and analyzed in a WSN. Such private information of concern may include payload data collected by sensors and transmitted through the network to a centralized data processing server. For example, a patient's blood pressure, sugar level and other vital signs are usually of critical privacy concern when monitored by a medical WSN which transmits the data to a remote hospital or doctor's office.

Privacy protection has been extensively studied in various fields related to WSN such as wired and wireless networking, databases and data mining. Nonetheless, the following inherent features of WSNs introduce unique challenges for privacy preservation in WSNs, and prevent the existing techniques from being directly transplanted:

Uncontrollable environment: Sensors may have to be deployed to an environment uncontrollable by the defender, such as a battle field, enabling an adversary to launch physical attacks to capture sensor nodes or deploy counterfeit ones. Sensor-node resource constraints: A battery-powered sensor node generally has severe constraints on its ability to store, process, and transmit the sensed data. As a result, the computational complexity and resource consumption of public-key ciphers is usually considered unsuitable for WSNs. This introduces additional challenges for privacy preservation.

Topological constraints: The limited communication range of sensor nodes in a WSN requires multiple hops in order to transmit data from the source to the base station. Such a multi-hop scheme demands different nodes to take diverse traffic loads. In particular, a node closer to the base station (i.e., data collecting and processing server) has to relay data from nodes further away from base station in addition to transmitting its own generated data, leading to higher transmission rate. Such an unbalanced network traffic pattern brings significant challenges to the protection of context-oriented privacy information. Particularly, if an adversary holds the ability of global traffic analysis, observing the traffic patterns of different nodes over the whole network, it can easily identify the sink and compromise context privacy, or even manipulate the sink node to impede the proper functioning of the WSN.

In hostile environments, it is particularly important to guarantee location privacy; failure to protect location-based information can completely undermine network applications. For example, in military applications, disclosure of the locations of soldiers due to nearby sensors communicating with the base station may allow an opposing force to launch accurate attacks against them. Providing location privacy in a sensor network is extremely challenging. On the one hand, an adversary can easily intercept the network traffic due to the use of a broadcast medium for routing packets. He can then perform traffic analysis and identify the source node that initiates the communication with the base station. This can reveal the locations of critical and highvalue objects (e.g., soldiers) being monitored by the sensor network. On the other hand, the resource constraints on sensor nodes make it very expensive to apply traditional anonymous communication techniques for hiding the communication from a sensor node to the base station.

Architecture Diagram

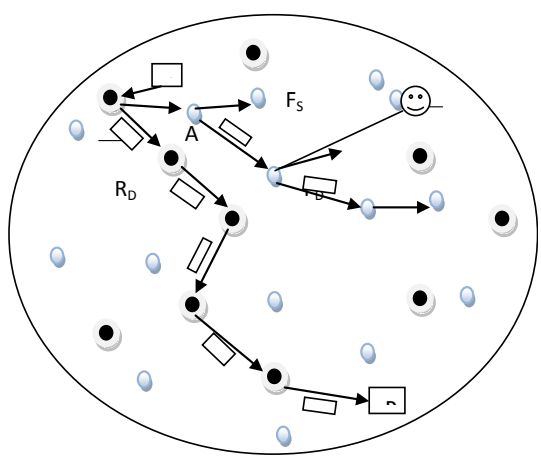


Fig. 1. Architecture in global eavesdropper.

2. Background

Prior work in protecting location privacy to monitored objects sought to increase safety period, which is defined as the number of messages initiated by the current source sensor before a monitored object is traced The coding technique [4] requires a source node to send out each packet through numerous paths to a destination to make it difficult for an adversary to trace the source. However, the problem is that the destination will still receive packets from the shortest path first. The adversary can thus quickly trace the source node using backtracking. This method consumes a significant amount of energy without providing much privacy in return. Kamat et al. describes two techniques for location privacy. First, they propose fake packet generation technique

[2] in which a destination creates fake sources whenever a sender notifies the destination that it has real data to send. These fake senders are away from the real source and approximately at the same distance from the destination as the real sender. Both real and fake senders start generating packets at the same time. This scheme provides decent privacy against a local eavesdropper. The other technique is called the phantom single-path routing, which achieves location.

Cyclic entrapment [5] creates looping paths at various places in the sensor network. This will cause a local adversary to follow these loops repeatedly and thereby increase the safety period. Energy consumption and privacy provided by this method will increase as the length of the loops increase. After the preliminary version of this paper was published, several source location privacy techniques have been proposed to deal with global eavesdroppers. Yang et al. propose to use proxies for the location privacy of monitored objects under a global eavesdropper [6]. The network is partitioned into cells where sensors in each cell communicate with the nearest proxy. Each cell sends traffic that follows an exponential distribution to its nearest proxy. The traffic will include dummy packets if real packets are not available. The proxies filter out dummy packets and send data to destination. The proxies also send dummy packets to estination if real event packets are not available. All packets are appropriately encrypted so that adversary is not able to distinguish between real and dummy packets. Proxy-based filtering and tree-based filtering schemes are proposed to position proxies. In addition, Shao et al. propose to reduce the latency of real events [7] without reducing the location privacy under a global eavesdropper. The technique makes sure that the adversary cannot determine the real traffic based on statistical analysis.

3. Backbone construction: Algorithm

Require: Each node has list of its neighbors

procedure BACKBONE (b,m)

Total coverage ←1

// first set in the L

id←GetMyId()

leader ← -1

//Local coverage ← Get NeighborCnt()

while true do

//Msg ← GetNextMsgFromQueue()

if TotalCoverage ≥ 2^b then

end if

if MsgType = NewMemberSelection then

if CheckNewMemberId(Msg)=Id then

//DestId←GetDestId(Msg)

SendElectionMsg(Id,DestId)

CollectVotes(Id,DestId)

CollectCoverageInfo(Id,DestId)

(ResultId,Coverage) ←Max_{id}(m)

if Valid(ResultId)=true then

//TotalCoverage ← TotalCoverage + Coverage

else

//(ResultId,Coverage) ← CollabrateRecursivelywithParent(Coverage)

if Valid(ResultId)=true then

TotalCoverage ← TotalCoverage + Coverage

Endif

End for

End while.

4. Result Analysis

We evaluate the performance of our new methods through simulations based on three criteria: delivery time, strength of privacy protection, and energy cost, which will be defined shortly. We compare our methods with single-path routing and two other location-privacy protection schemes: Phantom routing in [1] and DEFP in [2]. Single-path routing is used as the baseline scheme. Although Phantom routing is originally designed for protecting the location privacy of source nodes, to some extent it can also be used to protect the receiver's location privacy. We assign the random walk distance in the directed random walk phase of Phantom routing to be 10 hops. For DEFP, we use the default configuration settings in the original paper [2]. For LPR, the further/closer lists are calculated based on the Euclidean distances from the nodes to the receiver. When evaluating the strength of privacy protection, we first study the scenario where fake packets are not generated and then move to the scenario where fake packets are used. We will see that, with the significant energy overhead, fake packet injection is able to enhance the protection strength by two orders of magnitude or more.

Delivery Time

Delivery time is the time it takes a packet to move from its source node to the receiver under a certain routing protocol. In our simulations, it is measured as the average number of hops that packets from a selected source node traverse before reaching the receiver. The baseline single-path routing scheme has the smallest delivery time because the packets always follow the shortest path to the receiver. For other schemes, the packets may follow longer paths due to randomization introduced in the routing process.

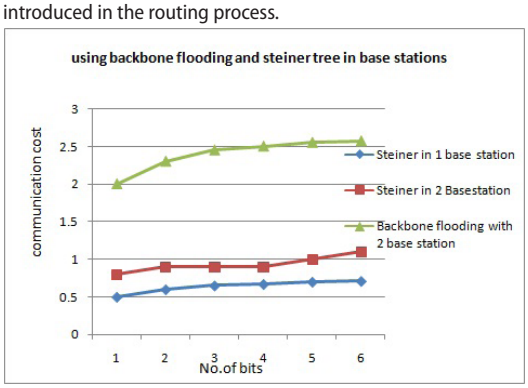


Fig.2.Comparison of sink-location privacy techniques in terms of communication.

5. Conclusion

There are a number of directions that worth studying in the future. In particular, in this paper, we assume that the global eavesdropper will not compromise sensor nodes; he only performs traffic analysis without looking at the content of the packet. However, in practice, the global eavesdropper may be able to compromise a few sensor nodes in the field and perform traffic analysis with additional knowledge from insiders. In particular, in this paper, we assume that the global eavesdropper will not compromise sensor nodes; he can only perform traffic analysis without looking at the content of the packet. However, in practice, the global eavesdropper may be able to compromise a few sensor nodes in the field and perform traffic analysis with additional knowledge from insiders. This presents interesting challenges for both of our approaches. In addition, we are also interested in the implementation of our methods on real sensor platforms and the experimental results from real sensor applications. This presents interesting challenges for both of our approaches. In addition, we are also interested in the implementation of our methods in real sensor platforms and the experimental results from real sensor applications.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002. | [2] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l Conf. World Wide Web (WWW '08), 2008. | [3] BlueRadios Inc., "Order and Price Info," http://www.blueradios. com/orderinfo.htm, Feb. 2006. | [4] B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov, "On the Value of a Random Minimum Weight Steiner Tree," Combinatorica, vol. 24, no. 2, pp. 187-207, 2004. | [5] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003. | [6] L. Eschenaur and V. Gligor, "A key-management scheme for distributed sensor networks," Proc. of 9th ACM conference on Computer and Communications Security, 2002. | [7] M. Spreitzer and M. Theimer, "Providing location information in a ubiquitous computing environment," Proc. of 14th ACM Symposium on Operating System Principles, 1993. |