Issue 4, Vol.2 (March 2014)
ISSN 2249-6149

IMPROVED APPROACH FOR LOCATION PRIVACY IN SENSOR NETWORKS AGAINST A GLOBAL EAVESDROPPER

[1]Reshma Francis, [2]Dr.Rasmi P.S

[1]Postgraduate Student, Toc H Institute of Science & Technology, Kochi
[2.] Professor, Toc H Institute of Science & Technology, Kochi

ABSTRACT

There are many security protocols for sensor network to provide confidentiality for the content of messages. But the contextual information which will be containing the source and sink locations usually remains exposed. This information can be exploited by an adversary and may even destroy the entire sensor network. The current most efficient mechanism for protecting contextual information is backbone flooding.In the current mechanism the backbone leader is being elected by an election mechanism. The node with maximum coverage will be elected as the backbone leader. This mechanism assumes that the backbone is created soon after the network is deployed also it does not consider about the chance of selfish behaviour for the backbone leaders. In this new method I am considering the availably as well as its coverage together, we send packets to a connected portion of the network, called the backbone. The sinks are located in the communication range of at least one backbone member so as the packets are only flooded among the backbone members, they can receive packets from any source in the field. When we are creating a backbone network we have to make sure that the backbone leader has a wide range of coverage moreover this backbone leader does not show selfish behaviour. Because this behaviour may lead to denial of service and hence the message may become unavailable for the intended sinks. Thus this new method provides a new mechanism by periodically conducting an election between the sensor nodes regarding the behaviour of the current backbone leader. And according to the result of the election a periodical change in the leader will be there.

Key words: sensor networks, location privacy.

INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed small, multifunctional, and resource constrained sensors that are self-organized to monitor the physical world [1]. Wireless sensor networks are used in applications like wildlife habitat monitoring, security and military surveillance, and target tracking where it is difficult to set up a wired network.

There are many security protocols for sensor network to provide confidentiality for the content of messages, but contextual information usually remains exposed. Contextual information contains critical information regarding the source and sink locations, these information can be exploited by an adversary to derive sensitive information. Attacks on these components can even destroy the entire network. Existing techniques defend the leakage of location information from a local adversary who can only observe network traffic in a small region. However, a stronger adversary, who has a global view of the entire network, can easily defeat these existing techniques. The current most efficient mechanism for protecting contextual information is backbone flooding.In the current mechanism the backbone leader is being elected by an election mechanism. The node with maximum coverage will be elected as the backbone leader. This mechanism assumes that the backbone is created soon after the network is deployed also it does not consider about the chance of selfish behaviour for the backbone leaders. In this new method I am considering the availably as well as its coverage together, we send packets to a connected portion of the network, called the backbone. The sinks are located in the communication range of at least one backbone member so as the packets are only flooded among the backbone members, they can receive packets from any source in the field. When we are creating a backbone network we have to make sure that the backbone leader has a wide range of coverage moreover this backbone leader does not show selfish behaviour. Because this behaviour may lead to denial of service and hence the message may become unavailable for the intended sinks.

Wireless communication is always open in nature making it easy for attackers to eavesdrop or inject data packets in a sensor network .Sensor networks are usually deployed in open areas, where unattended sensor nodes lack physical protection, whereas other wireless networks composed of mobile devices such as laptops and PDA's with human presence is difficult to attack. This means attackers will experience much fewer obstacles when attacking a sensor network.

Privacy of sensor networks can be classified into two categories content privacy and contextual privacy. The risks on content privacy arise due to the ability of adversaries to observe and manipulate the content of packets sent over a sensor network. This type of problem is countered by encryption and authentication. However, even after applying strong encryption and authentication mechanisms, wireless communication media still reveal contextual information about the traffic carried in the network. For example, an intruder can deduce sensitive information from a sensor network by eavesdropping and analyzing the traffic patterns. In particular, the location information regarding the sender and receiver can be extracted based on the direction of wireless communications.

For applications like military surveillance, eavesdroppers have strong incentives to listen on network traffic to obtain valuable intelligence. Abuse of such information can cause monetary losses or endanger human lives. To protect such critical details, researchers in sensor network security have focused considerable effort on finding ways to provide basic security services such as authentication, integrity, confidentiality, and availability. Though these are critical security measures, they are insufficient in many applications. The traffic patterns of sensors can, by themselves, reveal the information regarding the context, which can disclose the location information of critical components in a sensor network. For example, in the Panda-Hunter scenario [15], a sensor network is deployed to track endangered giant pandas in a bamboo forest. Every panda has an electronic tag that emits a signal that will be detected by the sensors in the network. A sensor that detects this signal, the source sensor, then sends the location of pandas to a data sink (destination) with help of intermediate sensors. An adversary (the hunter) may use the communication between sensors and the data sinks to locate and then capture the monitored pandas.

In general, any target-tracking sensor network is vulnerable to such attacks. As another example, in military applications, the enemy can observe the communications and locate all data sinks (e.g., base stations) in the field. Disclosing the locations of the sinks during their communication with sensors may allow the enemy to precisely launch attacks against them and thereby disable the network.

In hostile environments location privacy is, very important. If there is any failure to protect such information it can completely subvert the intended purposes of sensor network applications .Thus, we need to develop location privacy measures to prevent the adversary from determining the physical locations of source sensors and sinks. These methods have to be energy efficient but energy lifetime of battery-powered sensor nodes is limited. And also the communication in sensor networks is much more expensive than computation, we analyze the communication cost to measure the energy consumption of our protocols.

Providing location privacy in a sensor network is challenging, because, an intruder can easily intercept network traffic due to the use of a broadcast medium for routing packets. He can extract information from packet transmission like time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. And also, sensors usually have limited processing speed and energy supplies. Traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks are very expensive. Thus we need to find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes. Recently, a number of privacy-preserving routing techniques have been developed, but most of them are designed to protect against an adversary network at a time. A highly motivated adversary can easily defeat these schemes. For example, the adversary could deploy his own set of sensor nodes to monitor the communications in the target network. This is especially true in a military or industrial spying context, where the intruder has strong, potentially life-or-death, incentives to gain as much information as possible from observing the traffic in the target network. The adversary can easily infer the locations of monitored objects and sinks by having a global view of the network traffic. A region in the network with high activity should be close to a sink, and a region where the packets originate should be close to a monitored object

RELATED WORK/SURVEY

In recent years, wireless sensor networks (WSNs) have drawn considerable attention from the research community on issues ranging from theoretical research to practical applications. The basic characteristics of wireless sensor networks such as resource constraints on energy and computational power, have been defined well .The critical privacy concern on information being collected, transmitted, and analyzed in a WSN has received less attention .Such private information of concern may include payload data collected by sensors and transmitted through the network to a centralized data processing server.

Sensor networks were deployed to monitor valuable assets. In many scenarios, an adversary may be able to back trace message routing paths to the event source, which can be a serious privacy breach for many monitoring and remote sensing application scenarios. The ability of different routing protocols to obfuscate the location of a source sensor, the several variations of flooding-based and single-path routing techniques, and found that none of these protocols are capable of providing source location privacy. To achieve improved location privacy and the routing techniques called phantom routing.

Phantom routing techniques were desirable since they only marginally increase communication overhead, while achieving significant privacy amplification [4].

Key establishment in sensor networks is a great problem because asymmetric key cryptosystems are unsuitable for use in resource constrained wireless sensor nodes because the nodes could be physically compromised by an eavesdropper. First, in the q-composite keys scheme, trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key pre-distribution's strength against weak attacks. Second, in the multipath-reinforcement scheme, to strengthen the security between any nearby nodes by, leveraging the security of other links. Finally, to present the random pairwise keys scheme, this method perfectly preserves the secrecy of the rest of the network when any node is compromised and also enables node-to-node authentication and quorum-based revocation [3]

Privacy Grid [2] framework which allows users to express their privacy requirements in terms of location hiding and QoS (Quality Of Service) measures to control query processing overheads. Privacy Grid mechanisms for processing anonymous location queries is provided. First, it provides a location privacy protection preference profile model, called location P3P, Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment, Privacy Grid incorporates temporal cloaking into the location cloaking process to further increase the success rate of location anonymization. The extensive experimental evaluation results and show that compared to existing grid cloaking approaches such as, our dynamic grid cloaking algorithms provide much higher anonymization success rate and yet are highly efficient in terms of both time complexity and update cost

Prior work that has focused on securing the routing between sensor nodes has assumed that the monitored objects are sufficiently powerful to defend itself against security threats. This considers strategies for securing the sensor network against a variety of threats that can lead to the failure of the base stations, which represents a central point of failure. Initially, multipath routing to multiple destination sink is analyzed as a strategy to provide tolerance against individual base station attacks and/or compromise. Then, confusion of address and identification fields in packet headers using hashing functions is explored as a technique to confuse the eavesdropper about location of the base station .Third, periodically changing the location of the base station in the network topology is studied as a means of enhancing resiliency and mitigating the scope of damage[5]

PROPOSED STRATEGY

In the proposed technique we send packets to the backbone leader, instead of sending them directly to a few sinks. There will be a backbone, a connected portion of network and for each backbone there will be a backbone leader .The packets are only flooded among the backbone members, and the sensors that belong to this backbone will only receive the packets. The real sinks will be located in the communication range of at least one backbone member, they can receive packets send from any source through their corresponding backbone leaders Clearly, for a global eavesdropper, the sink could be anywhere near the backbone. We assume that the backbone is created soon after the network is deployed and that the adversary does not eavesdrop until the backbone is created. The main component of backbone flooding is the construction of the backbone. The sinks are located in the communication range of at least one backbone member so as the packets are only flooded among the backbone

members, they can receive packets from any source in the field. When we are creating a backbone network we have to make sure that the backbone leader has a wide range of coverage moreover this backbone leader does not show selfish behaviour. Because this behaviour may lead to denial of service and hence the message may become unavailable for the intended sinks. Thus this new method provides a new mechanism by periodically conducting an election between the sensor nodes regarding the behaviour of the current backbone leader. And according to the result of the election a periodical change in the leader will be there.

Once backbone construction is complete, the source sensor just needs to communicate with the nearest member of the backbone. After a member receives the data, it will flood the data in the backbone. The real sink can always receive every packet. Based on the backbone creation algorithm, we can see that from the attacker's point of view, the real sink could be anywhere in the communication range of the backbone.

.

ALGORITHMS

Backbone construction

Require: Each node has list of its neighbors
1: procedure BACKBONE(b;m)
2: TotalCoverage ← 1 . //first sensor in the set L
3: Id ← GetMyId()
4: Leader← -1
5: LocalCoverage← GetNeighborCnt()
6: while true do
7: if TotalCoverage $\geq 2^b$ then
8: EXIT
9: end if
10: Msg← GetNextMsgFromQueue()
11: if MsgType= NewMemberSelection then
12: if CheckNewMemberId(Msg) = Id then
13: DestId ←GetDestId(Msg) .

Identification of sink

14: SendElectionMsg(Id,DestId)
15: CollectVotes(Id,DestId)
16: CollectCoverageInfo(Id,DestId)
17: (ResultId,Coverage) ← $Max_{Id}(m)$
18: if Valid(ResultId)= true then
19: TotalCoverage ← TotalCoverage +Coverage
20: else
21: (ResultId,Coverage)
Backtrack(Coverage,ResultId,m)
22: if Valid(ResultId)= true then
23: TotalCoverage ← TotalCoverage + Coverage

24: else
25: EXIT

// Cannot find more sensors to cover

26: end if
27: end if
28: NotifyNewMember(ResultId,TotalCoverage)
29: end if
30: else if MsgType(Msg)=ElectionRequest then
31: if Leader= -1 then
32: SenderId ← GetSenderId(Msg)
33: SendVote(SenderId)
34: Leader= SenderId
35: end if
36: else if MsgType(Msg)= CoverageInfoRequest then
37: SendCoverageInfo(LocalCoverage)
38: else if MsgType(Msg) = AcceptMessage then
39: LocalCoverage ← LocalCoverage -1
40: end if
41: end while
42: end procedure

For a given sensor i, let maxi(m) be a function that examines i's neighbors and outputs the ID of the neighbour that covers the maximum number of uncovered sensors. It also returns the number of sensors that the newly identified sensor covers. If this maximum number is less than m, the algorithm instead outputs $\perp$. The algorithm produces a connected backbone network at each step. We assume that each sensor has the list of its neighbors. Let L be the set of IDs of the backbone members. L is initially empty. We begin by adding a sensor that has the real sink in its range. We now describe this algorithm from perspective of a sensor that sends an election message and then from the perspective of a sensor that receives this message.

Every new sensor v added to the set L will send an election message to find the number of uncovered sensors each neighbour can cover. If maxv(m) outputs a valid sensor ID and the coverage of this node, the ID of this node will be added to L. The newly added sensor will then execute the same algorithm. If maxv(m) =$\perp$, v will collaborate with existing nearby backbone members to find a usable sensor using Algorithm 2. The backbone is a tree structure with backbone members as the tree nodes. During the collaboration, the sensor will need to get information from its parent to find a node that can cover at least m nodes. This collaboration could continue to next level of ancestors if such a node is not known to the immediate parent. This backtracking process continues until a sensor meeting the required constraints is found. If a sensor that can cover at least m uncovered sensors is unavailable, a sensor that covers the maximum number of uncovered sensors is used.

Backtrack procedure

1: procedure BACKTRACK(Coverage,Id,m)

2: ResultId ← Id
3: Max ← Coverage
4: LocalMaxId ← -1
5: CollectCoverageInfo(GetMyId(),NULL)
6: (LocalMaxId,Max) ← MaxId(m)
7: if Max≥ m then
return LocalMaxId.Max
8: else if Max < Coverage then
9: ResultId =LocalMaxId
10: Max= Coverage
11: end if
12: for EachUnvisitedNeighborBKMember do
13: (Id,Coverage)= Backtrack(Max, ResultId,m)
14: if Coverage≥ m then
15: ResultId= Id
16: Max= Coverage
17: break
18: else if Coverage > Max then
19: Max =Coverage
20: ResultId =Id
21: end if
22: end for return ResultId,Max
23: end procedure

The beginning and termination of the backtracking process depends on the value of m. A value of m ≤ 1 would mean that backtracking would start only if v cannot find any neighbor that can cover at least one uncovered sensor. If m has a value greater than the number of neighbors any sensor could have, then the backtracking process would ensure that the sensor that covers the maximum number of uncovered sensors is selected. Intuitively, this would mean that an increase of m would help in covering more sensors with the help of fewer backbone members. However, more energy will be consumed to form a backbone for a large m due to more backtracking steps.

CONCLUSION

All the previous works on location privacy in sensor networks assumed a local eavesdropper. This assumption is unrealistic given a well motivated adversary. A highly motivated adversary can easily eavesdrop by compromising the existing techniques .In this paper, I have formalized the location privacy issues under a global eavesdropper and estimated the minimum average communication overhead .To achieve a given level of privacy the backbone leader is periodically updated considering the selfish behavior. This new technique will provide location privacy to objects and sinks against a global eavesdropper.

REFERENCE

[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] Chan.H, Perrig.A, and Song.D, "Random Key Predistribution Schemes for Sensor Networks," Proc.IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003.
[4] Kamat.P, Zhang.Y, Trappe.W, and Ozturk.C, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. Int'l Conf. Distributed Computing Systems (ICDCS '05), June 2005.
[5] Deng.J, Han.R, and Mishra.S, "Enhancing Base Station Security in Wireless Sensor Networks,"Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.
[6] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.
[7] J. Deng, R. Han, and S. Mishra, "Intrusion Tolerance and Anti- Traffic Analysis Strategies for Wireless Sensor Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '04), June 2004.
[8] J. Deng, R. Han, and S. Mishra, "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks," Pervasive and Mobile Computing J., Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.
[9] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS '02), Nov. 2002.
[10] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private Queries in Location Based Services: Anonymizers are not Necessary," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD'08),2008.