Identification of Misbehaviors and Packet Loss in Mobile Ad hoc Network

Vijayakumar R[#1], Muralidharan R[#2], Dhanarasan P[#3]

[#] *Department of Computer Science and Engineering, Muthayammal Engineering College, Namakkal, Tamilnadu, India*

[1]r.vijay155@gmail.com

[2]muralidharan.cse2010@gmail.com

[3]getdhanarasan@gmail.com

Abstract— **There is chances like a data distributor had given his sensitive data to a set of trusted agents. These agents can be called as third parties. There are chances that some of the data is leaked and found in an unauthorized place. This situation is called IDS. In existing case, the method called *watermarking* is using to identify the leakage. Or also uses the technique like injecting fake data that appears to be realistic in the data. We propose data allocation strategies that improve the probability of identifying leakages. In enhancement work we include the investigation of agent guilt models that capture leakage scenarios.**

Keywords— **Web service, distributed system, discover, Hamlet framework, Skewness.**

I. 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[1]. What has received less attention, however, is the critical privacy concern on information being collected, transmitted, and analyzed in a WSN. 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. 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 multihop scheme demands different nodes to take diverse traffic loads. 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.

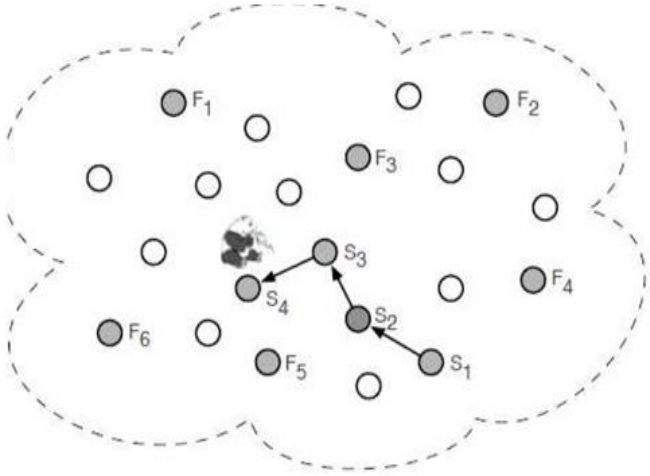

Fig. 1 Architecture in global eavesdropper

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. This can reveal the locations of critical and high value 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.

II. BACKGROUND WORK

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 [2] 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 [3] 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.

This contains number of cells to uses looping with some dummy packets in sensor networks. Cyclic entrapment [4] 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 [5]. 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 estimation 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 [6] 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.

III. BACKBONE CONSTRUCTION: ALGORITHM

Require: Each node has list of its neighborsprocedure
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 ≥ 2b 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)←Maxid (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.

IV. RESULT AND ANALYSIS

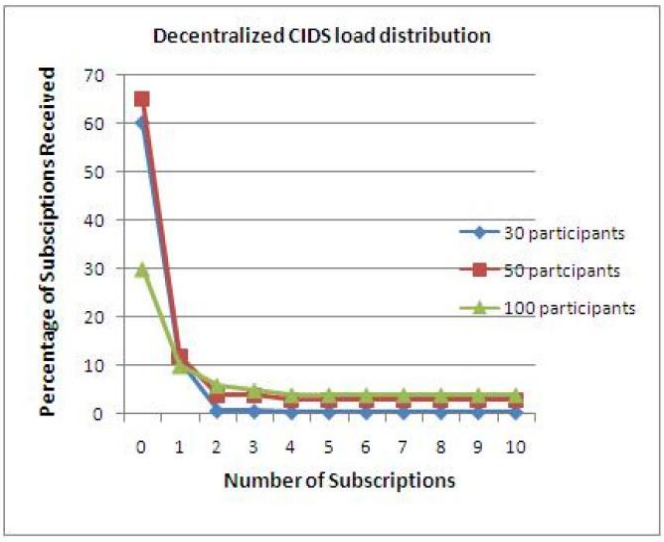

Fig. 2 CIDS percentage of load subscriptions

The proposed two-stage alert correlation scheme equipped with the probabilistic threshold estimation achieves significant advantage in detection rate over a naive threshold selection scheme for stealthy attack scenarios. The 98% confidence interval scheme gains a high *Detection Rate* without significant increase in the number of messages exchanged. Our results demonstrate that by using this probabilistic confidence limit to estimate the local support threshold in our two-stage architecture, we are able to capture most of the variation between different sub networks during a stealthy scan.

Subscription Delay (SD), which represents the time required for the participants to subscribe to each suspicious IP address on the responsible destination node, *i.e.*,

$$SD = Message\ Routing\ Delay + Message$$

Information Correlation Time (ICT), which denotes the process time required for correlating the subscription message on the destination node. *i.e.*,

$$ICT = Message\ Queueing\ Time + Data$$

Load Balancing, the load on each node in terms of the number of subscription requests that are received.

V. Conclusions

In a perfect world, there would be no need to hand over sensitive data to agents that may unknowingly or maliciously leak it. And even if, hand over sensitive data, in a perfect world, distributor could watermark each object so that distributor could trace its origins with absolute certainty. However, in many cases, Distributor must indeed work with agents that may not be 100 percent trusted, and may not be certain if a leaked object came from an agent or from some other source, since certain data cannot admit watermarks. In spite of these difficulties, it have shown that it is possible to assess the likelihood that an agent is responsible for a leak, based on the overlap of his data with the leaked data and the data of other agents, and based on the probability that objects can be "guessed" by other means. This model is relatively simple, but we believe that it captures the essential trade-offs. The algorithms we have presented implement a variety of data distribution strategies that can improve the distributor's chances of identifying a leaker. We have shown that distributing objects judiciously can make a significant difference in identifying guilty agents, especially in cases where there is large overlap in the data that agents must receive.

References

[1] BlueRadios Inc., "Order and Price Info," http://www.blueradios.com/orderinfo.htm, Feb. 2006.

[2] 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.

[3] 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.

[4] 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.

[5] L. Eschenaur and V. Gligor, "A key-management scheme for distributed sensor networks," *Proc. of 9th ACM conference on Computer and Communications Security*, 2002.

[6] M. Spreitzer and M. Theimer, "Providing location information in a ubiquitous computing environment," *Proc. of 14th ACM Symposium on Operating System Principles*, 1993.

