International Journal of Information Technology and Knowledge Management (ISSN: 0973-4414)
July-December 2012, Volume 5, No. 2, pp. 458-462

A COMPARATIVE STUDY OF TRAFFIC PADDING SCHEMES TO PREVENT TRAFFIC ANALYSIS IN SENSOR NETWORKS

Pooja Sharma
Research Scholar, Singhania University, Pacheri Bari, Dist. Jhunjhunu, Rajasthan
poojasharma161@gmail.com

Abstract: Wireless networks are envisioned to consist of large number of inexpensive and small nodes with sensing, data processing, and communication capabilities which are densely deployed in a region of interest and collaborate to accomplish a common task. One main challenge in design of these networks is their vulnerability to security attacks. However, there are various techniques exists in the literature like cryptography, stenography which are basically used to detect, and to protect the information from being detected by an attacker. But the experience shows, there are various overheads involved in their implementation like exchange of secret keys etc. So, in this paper we examine the role of traffic padding schemes in a sensor network which is concerned with protecting the user interest from being accessed by an attacker. To achieve the goal, there are two traffic padding schemes available, namely, source padding and link padding. We demonstrate that a link padding scheme can achieve better performance than a source padding scheme with lower power dissipation.
Keywords: Sensors Networks, Traffic padding, Traffic pattern..

1. Introduction

Knowledge about the number and length of messages between nodes may enable an opponent to determine who is talking to whom. This can have obvious implications in a military conflict. Even in commercial applications, traffic analysis may yield information that the traffic generators would like to conceal. Traffic analysis is a security attack that an intruder observes network traffic in order to infer sensitive information about the applications and/or the underlying system.

Traffic analysis is harmful because significant information about operation modes can be inferred by appropriately monitoring the pattern of traffic. This form of traffic analysis can, for example, uncover the location of command centers, or detect covert information flows to or from apparently non-involved parties [4]. It is therefore important to develop means to render traffic analysis efforts ineffective by using various techniques like network layers are encrypted. But, it is still possible in some circumstances for an attacker to assess the amount of traffic on a network and to observe the amount of traffic entering and leaving each end system. Countermeasure to this type of attack is traffic padding. We limit the interest of the adversary to the payload traffic rate, that is, the rate at which payload traffic is exchanged between protected networks. Therefore, we need to properly insert (additional) packets (called padding packets) into payload packet streams to camouflage them . In other words, Traffic padding means that some necessary dummy packets are injected into the network which is used to hide the traffic pattern.

Our study is based on a specific application, i.e. hiding user interests in a multi-task sensor network. In such a network as user changes interest, the traffic pattern in the network changes accordingly which provides linking information to an eavesdropper. We suggest for hiding the user's current interest by presenting a temporally constant traffic pattern. To achieve the goal, there are two traffic padding schemes available, namely, source padding and link padding.

2. Hierarchical Sensor Network

Figure1 demonstrates the network architecture .It is a three layer hierarchical network architecture, which consists of three types of sensor nodes : Low-power "Sensor Nodes (SN), Higher-power "Forwarding Nodes (FN), "Access Points (AP)", or called "Base Stations (BS)".

- Low-power "Sensor Nodes (SN)" with limited functionality;
- Higher-power "Forwarding Nodes (FN)" that forward the data obtained form sensor nodes to upper layer;
- Access Points (AP), or called "Base Stations (BS)"that route data between wireless networks and the wired infrastructure.

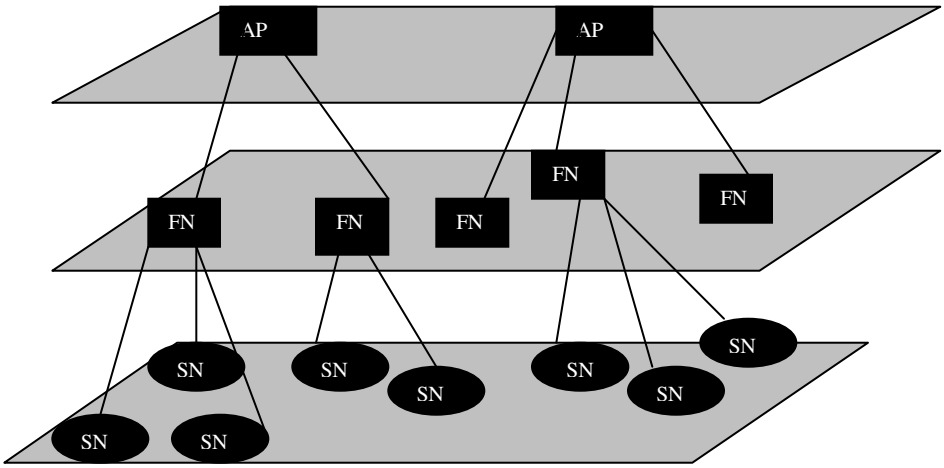

Figure 1: Architecture of a Hierarchical Sensor Network

SNs can be application specific (e.g., temperature sensors, pressure sensors etc.). They are deployed in clusters at strategic locations for surveillance and are controlled by a higher layer node, the FN. For each cluster of SNs, there is one FN, which serves as cluster head. An FN processes the data streams it receives from the SNs within the cluster. We assume the FNs are trustful and won't be compromised. We also assume the APs are trustful, otherwise the adversary can inject any data without been detected. Each FN has two wireless interfaces, one communicates with lower layer nodes (SNs), which belong to its management, and the other connects to higher layer nodes – APs. APs are located on the highest layer in a wireless APs provide multi-hop routing for packets from SNs and FNs within radio range, in addition to routing data to wired networks. This hierarchical network can also be considered as a distributed information aggregation system. SNs gather information and report to its FN. Based on the information collected from SNs. FNs compute the aggregation result and commit the information to APs. However, since SNs may be compromised and report fake information, it is important for FNs to verify the correctness of the information collected from SNs. Similarly, it is also desired

that APs possess the ability of verifying the committed information. network, and have both wireless and wired interfaces.

2.1 Problem Domain

In this section, we explain the user security goal which is the flow of traffic in the FN, that will change as the users current interests change. We take an assumption where we have a sensor network which consists of N number of FNs. Each senor node is an application specific means each node collecting the data for their respective tasks. Each task depicts a unique user interest. For user interest y, we assume that the rate at which FN x generates data is $g_x^y, x = 1, 2, \cdots, N$. If the eavesdropper continuously observes the traffic pattern in the FN network, he can easily find out what the user's current interest is. In order to prevent the user's interest from being detected. The way is to present a constant traffic pattern in the FN network without worrying about what the current user interest is. Specifically, the FN x generates the data at a rate $max_y(g_x^y)$ all the time. If we observe the current user interest which is k and the corresponding data rate is lower than the maximal rate, then dummy data needs to be generated in order to increase the traffic load to an eavesdropper.

The dummy data rate generated by the user to fool the adversary is $max_y(g_x^y) - g_x^k$. For the security consideration, all data traffic must be encrypted such that an eavesdropper cannot determine the real data in the whole network at any given time. Therefore, even if transmitted packets are intercepted by an eavesdropper, the message contents encapsulated in the packets are not disclosed. Each dummy data which is generated at an FN is broadcasted into the entire network just like the real data packets and forwarded to the destination node. This approach is known as a source padding approach. The cost of transmitted the dummy data throughout the entire network is typically high. Now we will discuss another effective approach which is called a link padding approach.

Link padding [1] [2] is a common technique used to hide the traffic pattern. It is based on the generation of artificial load, i.e. cover traffic or dummy traffic on a super set of those links where application traffic, which we will call real traffic subsequently traverses. To fool the adversary all data traffic must be encrypted such that cover traffic or dummy traffic is not distinguishable from real traffic. However, for serving real traffic, the network bandwidth can be reduced by using the padding traffic. The service provided by link padding is path hiding, not bandwidth or latency guarantees as in on-demand bandwidth reservation schemes such as RSVP [3]. The link padding has the probability of reducing the dummy traffic cost overhead which we are facing in source padding approach. In link padding, each FN has to maintain a constant traffic load on all output links at all the time. If we observe the real traffic load on a link which is lower than the expected level, then the sender node should generate dummy traffic in order to make the traffic load equal to the expected level. Unlike source padding, each dummy packet traverses only one hop and is discarded by the receiver

3. Comparison between Two Approaches

Here we compare the source padding and the link padding by using the traffic patterns corresponding with two distinct user interests. The numbers which are in parenthesis shows the traffic generation rate, generated by each FN in units per second. The number on each link gives

the observed traffic rate on the link by an adversary in units per second. With source routing, each node maintains a constant traffic generation rate, which may be larger than needed by the current user interest.As shown in Figure 2(b), node FN A generates data at a rate of 6 units per second and if the current user interest is 3 as shown in Figure 2(a), then the half percentage of the total traffic load is generated by the dummy data in order to show the increased traffic load. Node A sends the data to the node C which acts as a cluster head which in turn forward all the data to the BS without making any difference between the dummy traffic and the real traffic.

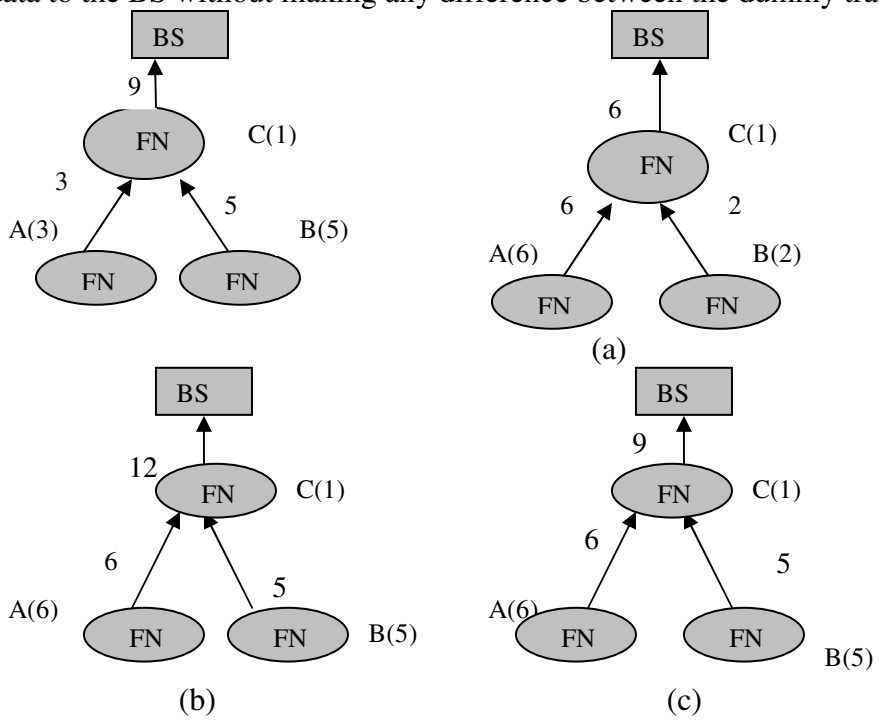

Figure2: (a) The Traffic Patterns corresponding with two distinct user interests (b) The cover traffic pattern with source padding; (c) The cover traffic pattern with link padding.

As we already explained, in link padding, dummy data is generated by each node at the link layer and therefore constant traffic load is maintained on a per-link basis. As shown in Figure 2(c), node C only forwards real traffic to the base station and discards dummy traffic received from node A and B, but it generates new dummy traffic to maintain a constant load on the link to BS, which is lower than in source padding.

4. Conclusion

In this paper we focused on hiding user interests in a multi-task sensor network. In such a network, as user interest changes, the traffic pattern in the network changes accordingly, which provides linking information to an eavesdropper. We suggest for hiding the user's current interest by presenting a temporally constant traffic pattern. To achieve this goal, there are two traffic padding schemes available namely, source padding and link padding. We compared the two approaches and determined that link padding generates new dummy traffic to maintain a constant load on the link to BS, which is lower than in source padding.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey Computer Networks (Elsevier), 38(4):393–422, Nov. 2002.

[2] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. Secure pebblenets. In Proc. of the 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pages 156–163, Long Beach, CA, Oct. 2001.

[3] D. Bertsekas and R.Gallager. Data Networks (Second edition). Prentice Hall, 1992.

[4] R.C.Summers, "Secure Computing," McGraw-Hill, 1997

[5] Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H-W., "Steganalysis on BPCS Steganography", Pacific Rim Workshop on Digital Steganography (STEG'03), July 3-4, Japan , 2003.

[6]Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, pp: 1043 – 1048, 2006.

[7] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[8] Tanveer Zia and Albert Zomaya, "Security Issues in Wireless Sensor Networks", IEEE.