International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 5 Issue 8, August-2016, Impact Factor: 1.544

Power – Aware Traffic Padding Schemes To Prevent Traffic Analysis in Ad Hoc Networks

Pooja Sharma

(Research Scholar), Kalinga University, Naya Raipur

ABSTRACT

Networks are designed to consist of large number of cheaper, smaller nodes with sensing, data processing, and communication capabilities, run in unattended mode, are densely used and collaborate to achieve a common mission. Wireless networks go beyond computer networks, contributing to the possibility of connectivity "everywhere and every time." One main challenge in design of these networks is their vulnerability to security attacks. Several cryptographic, stenographic and other techniques that are well known for detecting, preventing or reclaiming security attacks and for protecting information are used in the secure transmission of the different types of information over networks. However, the use of any security mechanism similar to the defense given, entails costs. In terms of increased resource use, higher system performance degradation, delaying transfer of packets or messages to another node and so forth, protection typically is accomplished at greater costs. In this paper we focus on providing network camouflaging services in wireless networks. Camouflaging of network is concerned in particular with hiding flow information, network traffic patterns and the transmitted data source/destination. We suggest to hide the user's current interest by presenting a temporally constant traffic pattern. For the reason, two traffic padding systems, namely the source padding and connection padding, are available. In terms of lifetime of the system and energy consumption, we compare the two methods. We show that a connection padding system can work better than a padding system with a longer system life and a lower power dissipation.

Keywords-**Sensors Networks, Network Camouflaging, Traffic padding, Traffic pattern, energy efficiency.**

INTRODUCTION

In recent developments in integrated circuits, a new generation of lightweight, cheap low-capacity sensors has been developed. Due to their economic and computation viability, a network of 100 000 sensors has the potential for various applications, including battle field control, protection and disaster management, both militarily and civilly. In the coming age of general computing, sensor networks are expected to play an important role. Safety in hostile environments is crucial to such networks, and safety problems remain a significant obstacle to the widespread deployment of such wireless networks. Many sensor networks track the environment actively and sometimes information other than the data monitored can be easily deduced.. Furthermore, wireless communication across sensor networks makes it possible for an adversary to eavesdrop and insert packets. Protection is a commonly used term covering authentication, integrity, confidentiality, non-repudiation, and anti-playback functionality. Various attacks are known to challenge the security, completeness and availability of information. The more reliance on network information is increased, the greater the probability of secure information being transmitted across networks.

CAMOUFLAGING FUNCTION OF NETWORK

Traffic analysis has evolved as a method for different users and environments. Classification clients, player classification[1], bot detection[1][2], and several other settings have been used to compromise anonymous communications. In certain environments only a small amount of information may be included in the observed traffic streams. (a) Packet data is normally inaccessible, it is encrypted; (b) header information is usually very restricted because the true traffic is either tunnel or the sender has changed header information properly. Only the timing information on the traffic is accessible

exclusively to the user after some initial filtering of the traffic (e.g. traffic from trustworthy sources and to ports, which do not make it possible to use it misuse themselves).

Traffic analysis can be avoided by camouflage of payload traffic, i.e. manipulation of the traffic to prevent an observatory from revealing its pattern and the operating status of the applications. Network camouflage refers particularly to the patterns of traffic and the source / destination of data transferred by hiding flow information. The essence of anonymous communication is to conceal the sender identity and/or the recipient identity from external observers. The opponent obtains knowledge about the flow by passive attack. Since eavesdropping is difficult to avoid, the most successful way to conceal information is to provide the eavesdropper with incorrect information. The false information sent to the eavesdropper deliberately acts as an envelope for the true information. One way of avoiding traffic analysis attacks is to "pad" the payload traffic, which is to insert dummy "packets"[3] properly into the payload stream to camouflage the actual payload status. The most common padding method used to monitor the sending of packets is by a timepiece, which works as follows: (a) Incoming Alice payload packets are put in queue on the padding node. (b) The timer is set to interrupt.

NEED FOR HIDING TRAFFIC PATTERN

In the field of network security, encryption historically played an important role. But it is a misunderstanding that one needs only to encrypt traffic in order to protect a network. With increased traffic volumes and the coded material beyond efficient cryptanalysis, we are turning our attention to and preventing traffic analysis. Traffic analysis is a security intrusion that an attacker observes to infer confidential details about apps and/or processes. Traffic analyses are dangerous as valuable information on operating modes can be obtained from adequate traffic pattern monitoring. Traffic analysis can be avoided by covering payload traffic, i.e. traffic manipulation so that its pattern is not associated with an observer or applications in operational status. The following steps should be incorporated in order to accomplish this:

• **Traffic padding:** The opponent's aim is to conduct traffic analysis and deduce important characteristics of the payload traffic transmitted over the unprotected network. The interest of the opponent is restricted to the payload ratio, that is the rate of exchange between protected networks of payload traffic. We have to insert (additional packages into payload streams (known as padding packages), so we can disguise them.

• **Host based traffic re-routing:** a packet can be sent to certain intermediate hosts during the host-based re-routing and then sent to its true purpose. The real traffic source and target can be hidden by means of sufficient encryption by means of host-based rerouting. Although the observer may receive an established host source address and a current traffic destination host address, the observer may or may not observe the true traffic source and destination.

This can make the job of traffic analysis considerably more complicated. To stop the study of traffic, we might need to redirect a traffic stream between two hosts through various paths traffic in order to disguise. Traffic padding means some dummy packets are need injections into the network or in other words a typical technique is traffic padding used to mask the pattern of traffic. In advance, two decisions must be taken the method of traffic padding: when and how to create dummy traffic It takes a lot of dummy traffic. Figure 4 illustrates the method of padding. As a result of the padding process, the padding and payload composition traffic is created (including traffic directly and redirected).

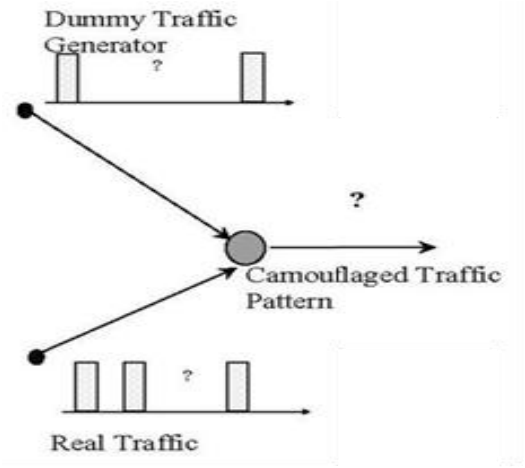

Figure 1: Process of traffic padding

The goal of the padding process is to establish the true pattern of transport comply as closely as possible with the camouflaged traffic pattern.

HERARCHICAL SENSOR NETWORK

The network architecture is shown in Figure 24. It consists of 3 different types of sensor nodes: low power hierarchic network architecture.

'Sensors Nodes (SN), 'Superior Nodes forwarding (FN),' 'Entry points' or 'Base Stations' (BS),' 'Base Stations'., small usable "Sensor Nodes (SN)" The SNs may be unique for use (e.g., temperature sensors, pressure sensors, video sensors, etc). They are deployed for tracking or monitoring applications in groups or clusters) in strategic locations. The SNs shall send the collected data to the local FNs. We assume that every SN contains the FN in its cluster directly. SNs therefore do not have the task of transmitting data. "Forward Nodes (FNs)" higher energy that transmits data received from sensor nodes to top levels; The path data between the wireless networks and the wired infrastructure, "Access Points (AP)," or "Base Stations (BS)."

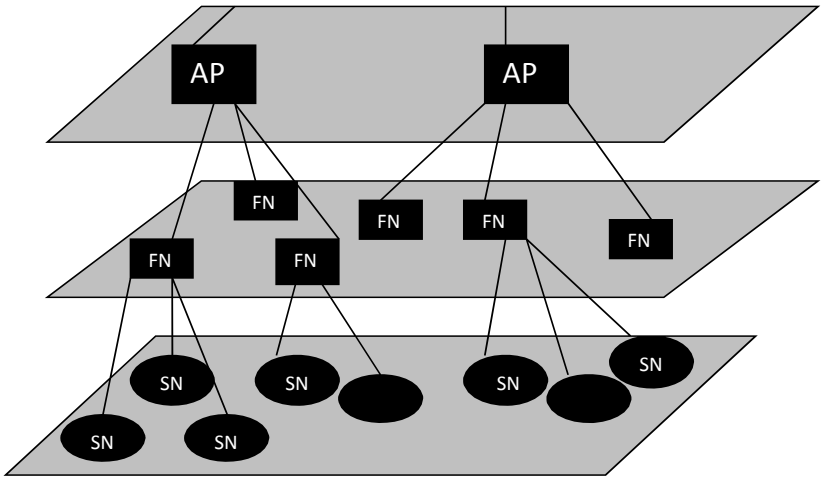

Figure 2 Sensor Network architecture

Unlike sensor nodes in ad-hoc flat sensor networks, sensor nodes in this hierarchy network's lowest layer do not provide their neighbors with multihop routing capability. A number of SNs are arranged as a group with a higher layer node, the FN, in charge. Each sensor node therefore communicates only with its FN and supplies information like reading the sensor to its FN. FNs are located on the sensor node layer in the second layer top and provide multi-hop routing for SNs or other FNs.

We presume that the FNs are confident and will be unaffected. Each FN has two wireless interfaces, with one communicating with SNs belonging to the lower layer Their management, and the other links Access Points to higher layer nodes. Access points (APs) or base stations have wireless interfaces and are located in one of the highest layers of the wireless network. The base station is the sink for all network FN data sources. It acts as a user-sensor-network interface. The FN network is used often to distribute user preferences through all FNs from the base station. In addition to routing data to wired networks, APs also provide multi-hop routing for radio packets from SNs and FNs. In addition, APs feature to relay wired network control information to FNs and SNs.

We also believe that the APs are trustworthy; otherwise the opponent may inject some information. Often a framework for distributed knowledge aggregation is a hierarchical network. SNs collect and report to their FN. On the basis of the data obtained from SNs, FNs determine the product of the aggregation and forward it to APs. But as SNs can be impaired and false information published, it is necessary for FNs to verify that the information gathered from SNs is accurate. Likewise, APs are also requested to have the capacity to verify the committed data. As mentioned above, SNs are not responsible for the transmission of data. Based on data obtained from SNs, the aggregation result is determined by FNs such that they consume more energy than SNs. Thus, due to wireless communication there is a need to conserve electricity. If the FN node releases the energy more quickly, the coverage for the regulated area that's going to be lost. We are researching the power-efficient routing algorithm of the FN network to extend the longevity of the FNs.

Domain problem

We describe in this section the user safety goal of the FN traffic flow. This is going to change with existing users shifting preferences. We assume that we have a network of sensors consisting of N numbers of FNs. Each senor node means that each node collects the data for its respective tasks. Each role represents a single interest for the consumer. We assume that the rate at which FN x generates data is g_x^y, x = 1, 2,• • •, N .. By monitoring the traffic pattern of the FN network continuously, eavesdropper can easily determine the current interest of the user. We would of course, be thinking of the following questions:

1. Is there a way to prevent eavesdropper from detecting the user's interest?
2. How much would the eavesdropper cost to hide consumer interests?

The response to the first issue is yes, we can pursue a way to avoid detecting the user's interest. In this way, the FN network provides a constant pattern of traffic without caring about the current user interest. In particular, the data at a rate $MAX_y(g_x^y)$ is always generated by FN x. If the current user interest k is observed and the corresponding data rate is below the max. rate, then stupid data must be produced to increase the traffic to an eavesdropper.

$MAX_y(g_x^y)$ —$g_x^{k\,k}$ is the dummy data rate the user produces to delude the opponent. All data traffic needs to be encrypted for security reasons, So that the exact data in the entire network is not decided at any point by an eavesdropper. Thus the message information found in the packets will not be revealed even though the transmitted packets are intercepted by the eavesdropper. All the stupid data that is generated on the FN, like real data packets, is transmitted to the entire network and forwarded to the target node. This is called a padding approach from a source. The transmission costs for dummy data are usually high across the whole network. Now we are going to talk about another efficient approach called connection padding.

A common technique for hiding the traffic pattern is connection padding. It is based on the artificial load generation i.e. on traffic cover or dummy on a super collection of those connections, which are later called real traffic. All data traffic must be encrypted in order to deceive the opponent so as not to differentiate between traffic or dumb traffic and actual traffic. The network bandwidth can however be decreased by using padding traffic to serve actual traffic. The service offered by link padding is track secret and not bandwidth or latency guarantees, as in reservation schemes for on-demand bandwidth such as RSVP[4]. The Linked padding[1][5] is likely to reduce the overhead cost of dummy traffic that we face in a source padding method. Link padding is based on the two observations: 1) the interest of the user is transmitted to all the networked FNs. If a FN is fitted with an eavesdropper, this scheme would not be useful. 2) The traffic cover may be given at the connection if the FN does not cooperate with the eavesdropper. On any output connection, each FN must maintain a constant traffic load . When observing the actual load of traffic on a connection below the expected level, a dumb traffic node should be created so that the load is equal to the anticipated level. In contrast to source padding, each fool packet only traverses one hop and is discarded by the recipient.

CONNECTION PADDING OPERATION AT A NODE

We use token-bucket based schemes in order to generate cover traffic as shown in Figure 3. The token bucket collects tokens, including coverage and actual traffic, at a rate that corresponds to the target traffic. If a token bucket receives a token, a packet would be sent from real traffic if the real traffic queue is not empty, and the actual traffic queue is deleted from a packet too. Otherwise as part of the cover traffic the node would give a padding packet. Just a token from the token bucket is removed in this situation. There are different kinds of attachment padding. Padding traffic is introduced into a connection in the conventional form, which we call "flap" or "constant connection padding".

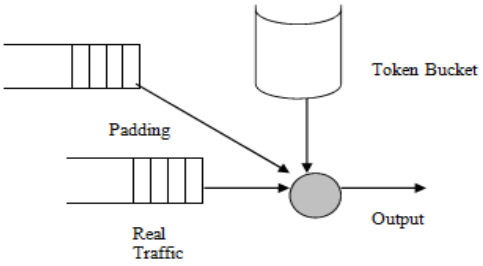

Figure3: Implementation of Token Bucket Connection Based Padding.

COMPARISION BETWEEN TWO APPROACHES

The source padding and connection padding are contrasted by using traffic patterns that fit two distinct user interests. The numbers in parenthesis show the frequency of output produced in units per second by each FN. On each connection, the number of adversaries per second gives the observed traffic rate on the link. Every node has a constant traffic generation rate with source routing which may be greater than the user interest required.

As shown in Figure 4(b), FN A node generates a data rate of 6 units per second and in Figure 4(a), if current user interest 3 is present, then dummy data generate a half percentage of the total load of traffic to display the increased load of traffic. Node A sends the information to the node C that functions as a cluster head and transmits all the information to the BS without differentiating between dummy and real traffic.

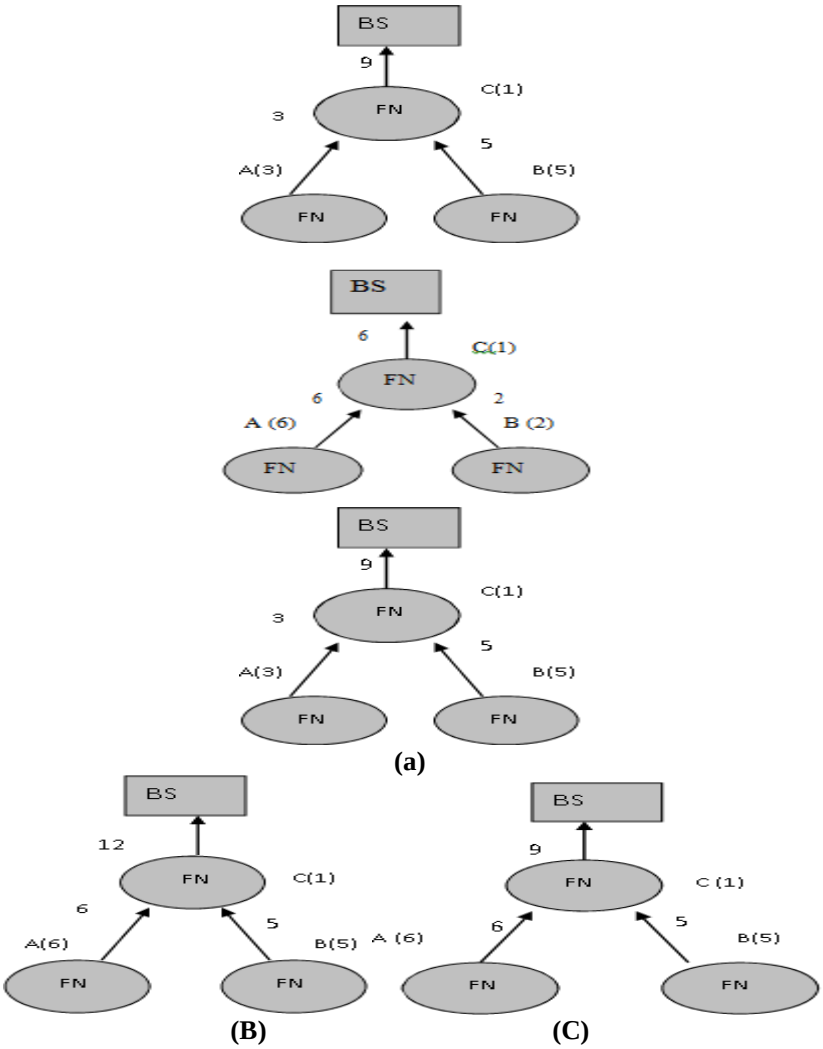

Figure 4: (a) Traffic patterns that are compatible with two separate user interests (b) the source padded cover traffic pattern; (c) the connection padding cover pattern.

As we have already mentioned, dummy data are created in the connection padding by every node on the link layer and thus traffic per link is maintained constantly. Figure 4(c) shows that node C only provides true traffic to the base station and Dummy reject node A and B traffic generates new dummy load, which is lower than in source padding, to maintain a continuous load on the BS connection. Padding traffic injected into the network contributes to higher energy consumption. The second is the total energy consumption, and two metrics are known to describe the energy consumption with and without traffic padding.

System Lifetime T: The lifetime of the system is the period of time, before at least one FN node is energized.

System Power Consumption R: average consumed energy per data unit given for its function. In R measurement, energy consumed by all nodes transmitting packet is taken into consideration. The choice of simultaneously optimizing the above two metrics will be reduced. In order to reduce energy consumption, there is a need for data traffic from the FNs to the base station to take minimum costs, as each node spends power not only on sensing and transmitting its own data, but also transmitting data from other sensors. At different rates, each node spends its energy based upon its network positions. The closer two nodes are the less energy is required to send and receive data between them, based on the FN models of power consumption. The node that is far from the base station decreases its energy more rapidly than other nodes. As a result, some nodes would have to handle higher transport loads compared to other nodes and use energy to minimize the life time of the system earlier than other nodes.

RESULTS

The results of the simulations are shown here. We have an Arbitrary Network consisting of a random number of FNs transmitted randomly on a square area of 1000m x 1000m and a base station at the centre of the area, the sink node. In order to transmit its relevant information, we presume that each node has a direct connection with the base station or any other node of the network. We set the transmission range of every node to 250m, so that each node is connected entirely to other nodes.

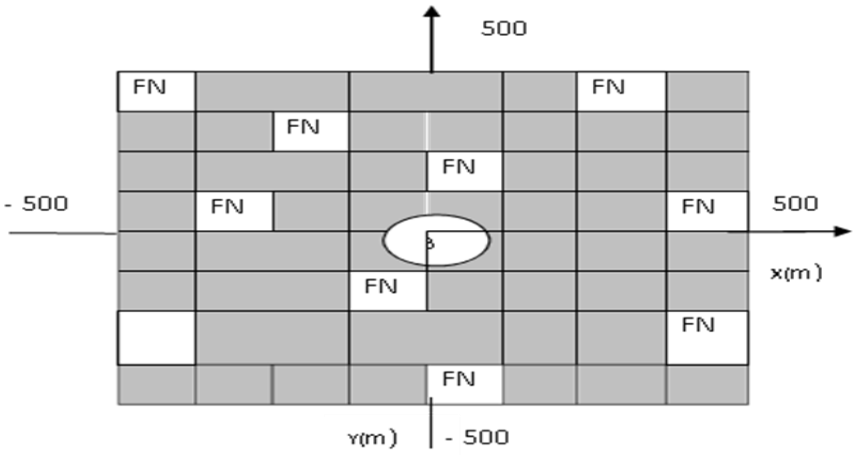

Figure 5: Network of Random FN

We are also interested in different users who can adjust during simulations. The initial energy of each FN is 50KJ. Each FN produces random data between 0 and 100b/s for every user's interest. We compare the output of connection padding and source padding Sparse network degradation with 10, 20,30,40,50. FNs number. To this end, the cumulative life of the system and the minimum systems dispensing for a given network have to be specified by a collection of patterns of traffic without padding. We assume that the same probability of being requested would apply to any user interest. First by considering various traffic loads in a 50FN network, shown in Figure 6, we compare connection padding and source padding.

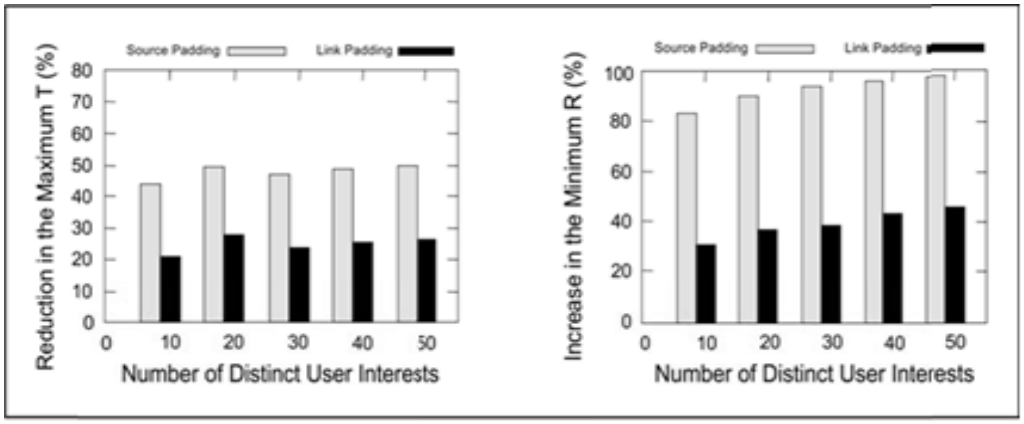

Figure 6: comparing connection padding and source padding under diff loads

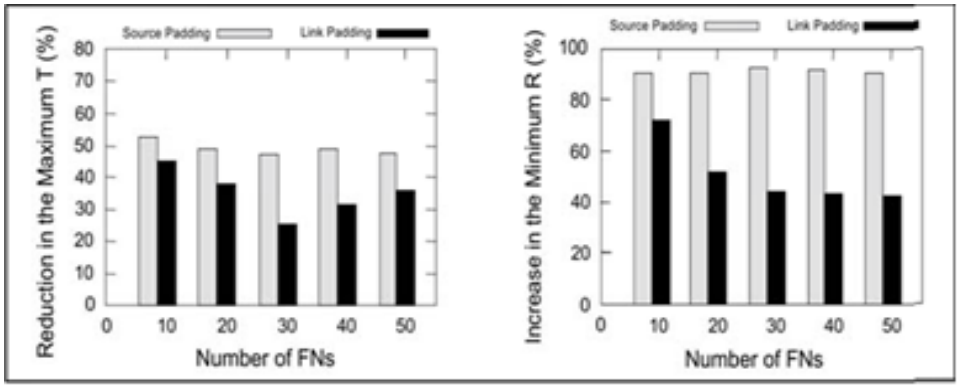

Figure 7: Connection padding and source padding for various network sizes Comparing

The number of interest rates ranges between 10 and 50. Each value is 10 simulation runs on average. Figure 6 indicates, depending on the number of users involved in the connection padding, that the overall lifetime of the device can be reduced by between 20 and 30 percent while the source padding can be reduced by 48 to 50. Source padding also indicates that the minimum device power dissipation is above 80%, while connection padding raises the system's power dissipation by 20%-40%, which is half of source padding. We therefore assume that the padding of the source causes a deeper level of output than the connecting padding. By using the different Network Sizes in Figure 7 we compare the connection padding and the source padding. The number of different user desires here is twenty. Average of ten simulation runs is shown by each value. When the network is limited, it is shown that connection padding and source padding is approximately similar because there are fewer separate paths from each FN to the base station. It is shown that In comparison, where there is a large number of separate paths, the data traffic from the same source is spread to the many different paths within the network. Obviously, the average traffic charge for each link will be lower if the vast numbers of different paths are available. We have therefore concluded that a connection padding approach will reduce the cover load on each connection.

CONCLUSION

In this paper we focused on providing network camouflaging services in wireless networks. Camouflaging of network is concerned in particular with hiding flow information, network traffic patterns and the transmitted data source/destination. We suggested to hide the user's current interest by presenting a temporally constant traffic pattern. For the reason, two traffic padding systems, namely the source padding and connection padding, are available. In terms of lifetime of the system and energy consumption, we compare the two methods. We show that a connection padding system can work better than a padding system with a longer system life and a lower power dissipation.

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]. D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus. Requirements For traffic engineering over MPLS. Internet RFC 2702, http://www.ietf.org/rfc /rfc2702.txt?number = 2702, Sept.1999.
[3]. R. Want, A. Hopper, V. Falcao, and A. Gibbons. The active badge location system. ACM Transactions on Information Systems, 10(1):91–102,1992.
[4]. D. Bertsekas and R. Gallager. Data Networks (Second edition). Prentice Hall, 1992.
[5]. 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.
[6]. [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.