Enhanced Energy Efficient Privacy Provisioning in WSN

MANJUSHA PANDEY,SHEKHAR VERMA
Indian Institute of Information Technology, Allahabad, India.
Email: rs58@iiita.ac.in ,sverma@iiita.ac.in

Abstract: - Privacy provisioning along with the core functionality of WSN including routing of the sensed data through predetermined optimized routes to the base station which produces pronounced traffic near the sink node adding up to the revelation of either location of direction of location of base station is one of the major research challenges in WSN. The proposed privacy provisioning scheme aims to optimize energy consumption for privacy provisioning in WSN. The traffic patterns may be disguised by introducing fake packets to the generated traffic of original data and a time to live parameter is introduced to execute lesser energy consumption. Earlier also many anti traffic analysis strategies have been proposed and implemented with the same objective But the inclusion of fake packets adds up communication overhead and higher energy consumption in the network as a whole. Hence the problem undertaken in the current research effort is to optimize the energy consumption at the node level for fake packet generation by using residual energy of each node. The energy optimization has been done using the two fold privacy provisioning *a)* generation of fake packets by the nodes having larger residual energy and avoiding nodes having residual energy less than a threshold value. *b)* The fake packet generated has an associated TTL (Time toLive)that can be constant or based on the residual energy of nodes.

Key-Words: -WSNs; wireless sensor networks; Privacy in WSN; Traffic analysis; energy efficiency.

1 Introduction

A Wireless Sensor Network [1] basically evolutions of adhoc networks are a self-configuring network. These networks consist of small sensor nodes communicating among themselves using radio signals. The tiny sensor nodes are generally deployed in large quantity to sense, monitor and understand the physical world for varied real life applications.WSN provide a bridge between the real physical world and virtual worlds of networks.

They provide the ability to observe the previously unobservable physical space at a fine resolution over large spatio-temporal scales. Wireless sensor networks have many a potential applications to industry, science, transportation, civil infrastructure, and security. Advances in precise fabrication techniques and nano technology enabled the evolution of tiny sensor nodes compared to its predecessors. In WSN the nodes are not only responsible for sensing and communication task, they are also capable of doing in-network data processing, data fusion and correlation tasks. Sensor networks consist of different types of devices as the sensors, seismic, acoustic, magnetic, thermal, infrared, etc. In WSNs, each node has a radio that provides a set of communication links to nearby nodes. By exchanging information, nodes can discover their neighbors and perform a distributed algorithm to determine how to route data according to the application's needs. Although physical placement primarily determines connectivity, variables such as obstructions, interference, environmental factors, antenna orientation, and mobility make determining connectivity a priori difficult. Instead, the network discovers and adapts to whatever connectivity is present. [2, 3] Security and privacy in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of deployment. The overall cost of the WSN should be as low as possible. Sensor nodes are susceptible to physical capture, but because of their targeted low cost, tamper-resistant hardware are unlikely to prevail. Sensor nodes use wireless communication, which is particularly easy to eavesdrop on [4].

Similarly, an attacker can easily inject malicious messages into the wireless network. [5] Advanced anti-jamming techniques such as frequency- hopping spread spectrum and metrics. Physical tamper proofing of nodes are generally impossible in a sensor network due to the requirements of greater design complexity and higher energy consumption. The use of radio transmission, along with the constraints of small size, low cost, and limited energy, make WSNs more susceptible to denial-of-

service attacks [6]. Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message, impersonating nodes etc. Security also needs to scale to large-scale deployments. Thus, a promising approach is to use more efficient symmetric cryptographic alternatives [7]. Instead, most security schemes make use of symmetric key cryptography. One thing required in either case is the use of keys for secure communication. [8] Managing key distribution is not unique to WSNs, but again constraints such as small memory capacity make centralized keying techniques impossible. Most current standard security protocols were designed for two-party settings and do not scale to a large number of participants [9].

There is a conflicting interest between minimization of resource consumption and maximization of security level [10]. A better solution actually gives a good compromise between these two. Since sensor nodes usually haveseverely constrained, asymmetric cryptography is often too expensive for many applications [11].

2 Issues and Challenges

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wireless sensor network is a special network which has many constraint compared to a traditional computer network.

a) Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks.

b) Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self configuration. Security schemes must be able to operate within this dynamic environment.

c) Hostile Environment

The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. crypto graphic keys). The highly hostile environment represents a serious challenge for security researchers.

d) Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient.

e) Immense Scale

The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tends to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

f) Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. *Unreliable Transfer:* Normally the packet based routing of the sensor network is connectionless and thus inherently unreliable. *Conflicts:* Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. *Latency:* The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

g) Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main cautions to unattended sensor nodes: *Exposure to Physical Attacks:* The sensor may be deployed in an environment open to adversaries, bad weather, and

so on. The probability that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network. *Managed Remotely:* Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues. *No Central Management Point:* A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile. Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

3 Problem Formulation

The nodes near the base station in a WSN clearly forward a significantly greater volume of packets than nodes further away from the base station, in the same manner that a river grows wider as it collects more water from its tributaries. An adversary can analyze the traffic patterns revealed in to deduce the location of the base station within the WSN's topology. Since the base station is a central point of failure, once the location of the base station is discovered, an adversary can disable or destroy the base station, thereby rendering ineffective the data-gathering duties of the entire sensor network.

The current research effort focuses on developing an anti traffic analysis privacy preservation mechanism that countermeasures against traffic analysis attacks [15] that seek to locate the base station, particularly against the rate monitoring and time correlation attacks. Aim is to restrict an adversary who is analyzing packet transmissions within its range, to analyze the maximum flow of traffic towards the base station. The overall objective is to have a uniform traffic within the network. In particular, our goals are:

• An adversary cannot find the data flow direction by analyzing the event generation by analyzing the statistical flow of data transmission.
• An adversary cannot find the data transmission direction by employing statistical analysis of the packet transmission rate of every node within its range.

A simple defense against plaintext observation is to encrypt each packet. However, if data packets are encrypted, but do not change hop by hop, then an adversary can still follow a given encrypted packet pattern towards its destination, which will often wind up at the base station. Following the path of encrypted packets can be defeated if each data packet is re-encrypted at each hop, thereby changing the appearance of each packet at each hop, e.g. by employing pair-wise key schemes. Even with hop-by-hop re-encrypted packets, an adversary can still deduce significant information that can reveal the base station's location by monitoring traffic volume, or by looking at time correlations. The act of transmitting itself reveals information to the attacker, regardless of whether packet contents can be inspected.

4 State of Art

Based Privacy preservation in sensor network differ a lot from the traditional networks as the sensor networks have different set of characteristics and solutions used in traditional networks are too burdensome for sensor networks. The adversary may track back origin of multi-hop communication in sensor networks as the radio transmission is over wireless medium this facilitates the adversary for the same [16]. Launch of physical attacks and node compromises by the adversary thus posing a menace to the whole wireless sensor networks is quiet evident due to the miniature size of the sensor nodes and very nature of the wireless communication environment. As we know a wireless sensor network is severely constrained by various resources as computation, storage, and wireless communication bandwidth and battery power. The adversary could monitor such activities of the sensor as the communication patterns to figure out the energy depletion or resource usage in order to spot the most vulnerable spots in the network and use them to attack the network as a whole [17].

A lot of work has been done to conceal the traffic patterns of WSN *Baseline and probabilistic flooding mechanisms* [18]were proposed with the basic idea for each sensor to broadcast the data it receives from one neighbor to all of its other neighbors. But the baseline flooding has a serious drawback that it needs a cache at every sensor node to store the packet that has already been received so that it can compare duplicate packets and discard them. [19] *Random walk mechanisms*: Phantom Routing is the most primitive random walk approach proposed; in this the data performs few steps of random walk followed by probabilistic flooding towards the base station. Introduced random delay due to random walk and flooding as well as overhead of redirecting

traffic randomly makes these schemes unuseful for real-time applications. [20] *Dummy data mechanism:* To enhance the location privacy of base station fake data packets can be introduced thus perturbing the traffic patterns. Short lived fake source was introduced for location privacy preservation of base station that sent out the fake packets with predetermined probability. But the major disadvantages of this dummy fake packet injection was that it added a lot of bandwidth and communication cost. [21]*Fake data sources mechanism:* To protect the identity of real source of packet one or more sensor nodes can simulate the behavior of real source to confuse the adversary. Though more fake sources ensure better protection of identity of real source these techniques also incur higher power consumption. Furthermore, the major challenge for the design of this technique is how to simulate the behavior of data sources without being detected. [22] *Routing with multiple parent:* To balance the traffic load between parent nodes and child nodes so that an adversary is not able to identify the nodes nearer to base station routing with multiple parents was introduced .A malicious node can claim a low levelvalue of parent node to attract traffic from other nodes, or it can use unfair media access control mechanisms to occupy the wireless channel.[23]*Routing with random walk:* Routing with random walk logically segments the sensor nodes into closer and farther lists based on hop count from the base station. To forward data a sensor node randomly selects next hop from anyone of the two lists thus adding randomness to traffic generation pattern. The primary drawback of these approaches is the amount of overhead incurred to simulate a source or to redirect traffic randomly and these schemes also introduce a delay in delivering the packets which may not be useful in real time applications. [24] *Deco-relating parent–child relationship by randomly selecting sending time:* To restrict the adversary from finding out the parent child relationship between two sensor nodes based on the short time interval between sending data by child node and receiving data by parent node, the time period of T can divided into m slots if there is one parent for (m-1) child nodes. Still a malicious node can claim a low levelvalue to attract traffic from other nodes, or it can use unfair media access control mechanisms to occupy the wireless channel.[25]*Hiding traffic pattern by controlling transmission rate:*high transmission rate at the sensor nodes near base station is evident as these nodes relay the data from sensors that are farther away from base station along with their own data, this also facilitates that revelation of location of base station to the adversary .To overcome this a technique was proposed to maintain uniform transmission rate by controlling delay of real data. This scheme is effective but has a serious drawback that the rate needs to be controlled at every sensor node but to implement this realistically every sensor node must have a buffer so that it can delay the packet and there is a uniform rate at every node. This also introduces delay in the network. [26] *Propagating dummy data:*Fake packlet injection was proposed to prevent the adversary from identifying real data transmission patterns but the scheme has a major limitation of assumption that the adversary could not differentiate between the real and fake data. The dummy data injection scheme although preserves privacy but it also consumes a lot of bandwidth and hence a higher communication cost.

5Energyefficient Privacy Preservation

To address the shortcomings of other mechanisms, a new technique was proposed called fractal propagation [27]. In this technique, several fake packets are created and propagated in the network to introduce more randomness in the communication pattern. When a node hears that its neighboring node is forwarding a packet to the base station, the node generates a fake packet with probability, and forwards it to one of its neighboring nodes. These fake packets spread out in the network and their transmission paths form a tree. In particular, the communication traffic is much more spread out than random walk. So even if an adversary can track a packet using time-correlation, he/she cannot track where the real packet is going. This is because he/she cannot differentiate between a real and a fake packet without knowing the encryption key.

The major drawback of the fractal propagation was that generation of fake packets may take toll over the energy consumption of the sensor nodes. Hence as an effort to improve the energy consumption overhead along with the efficient privacy preservation we propose a residual energy based fake packet generation in fractal propagation.

5.1 Fake Packet Generation

Fake packet generation in the earlier schemes was based on a constant probability because of which the energy consumption optimization was not possible in WSN. The following subsection details our scheme of fake packet generation based on the residual energy.

5.1.1 Residual Energy Based Fake packet generation

The effort is to make the probability of fake packet generation by the sensor node proportional to the residual energy of each sensor node. For the calculation of residual energy the following algorithm has been used .When a node hears that its neighboring node is forwarding a data packet it also generates a fake packet with probability. The probability $P_{er}$is dependent on the average energy of the neighbors' of the sensor node.

Thus after the initialization the average energy of the node is equal to the residual energy of the node and probability of fake packet generation by the node is set to the predefined threshold value represented by the P_t .This threshold value may be varied with the requirements and perquisites of privacy preservation in the network considering other network parameters like network lifetime optimization [28] and routing and application dependent parameters [29].

The notations used for implementation of residual energy fake packet generation in our energy efficient privacy preservation mechanism are:

E_{MAX} = MAXIMUM BATTERY CAPACITY OF A NODE

E_R = RESIDUAL ENERGY OF A NODE AT A PARTICULAR INSTANCE

E_{AVG} = AVERAGE ENERGY CALCULATED USING EAVG OF ITS NEIGHBORS

P_T = THRESHOLD PROBABILITY SET TO SOME PREDEFINED VALUE (0.6,0.2,0.4)

P_{MAX} = MAXIMUM FORWARDING PROBABILITY

$$P_{MA}= \frac{P_T+(1.0-P_T)*(E_R-E_{AVG})}{(E_{MAX}-E_{AVG})} ..(1)$$

P_{MIN} = MINIMUM FORWARDING PROBABILITY

$$P_{MIN}= P_T * \frac{E_R}{E_{AVG}} ..(2)$$

P_{EFR} = FAKE PACKET FORWARDING PROBABILITY

ALOGRITHM 1. CALCULATION OF AVERAGE ENERGY OF NEIGHBORS

1. INITIALLY
   $E_{AVG} = E_R$
2. NODE SENDS BECON TO ITS NEIGHBOURS
3. REPLY (E_{AVG}) TO N_X
4. CALCULATE NEW E_{AVG}= AVERAGE (RECEIVED E_{AVG}, E_R)
5. NOW E_{AVG}=NEWE_{AVG}

ALGORITHM2. CALCULATION OF MEAN ENERGY PROBABILITY FOR FAKE PACKET GENERATION

1. IF $E_{AVG} = E_R$ THEN $P_{EFR} = P_T$
2. ELSE IF ($E_R > E_{AVG}$) THEN $P_{EFR} = P_{MAX}$
   ELSE $P_{EFR} = P_{MIN}$

If the residual energy of the node is greater than the average energy of its neighbor nodes then the probability of fake packet generation is set to be maximum for the current node else it would be set to the minimum value.

The maximum and minimum probabilities for fake packet generation by the nodes could be calculated as with the following algorithm based on the maximum energy of the current node the predefined threshold probability value for the entire network and average energy of the neighbor nodes of the current node.

For calculation of average energy the node sends beacon to its neighbor nodes on receiving the average energy values from neighbor nodes the node calculates its own average energy as the average of the received average energy of its neighbors' and its own residual energy. Again to control the propagation range of the fake packets, the newly generated fake packet contains a TTL (time to live) parameter with value L.

5.1.2 TTL (Time To Live) for Fake packet generation

L is a constant that is known to all nodes, so an adversary cannot flood the whole network by sending fake packets with length parameter higher than .When a node receives a fake packet, it decrements its TTL value by 1. The value of TTL has to be greater than zero, whenever any node forwards the fake packet to one of its neighboring nodes.

If the value for TTL parameter is zero, the node stops forwarding of the fake packet it had received. In addition, when a node hears that its neighboring node is forwarding a fake packet to someone else with length value l (l < L), it generates and forwards another fake packet with probability P_{er} and length value $l - 1$. These fake packets spread out in the network and their transmission paths form a tree. Suppose a node has x neighboring nodes on average. Let $P_f = P_{er} * x$ and f(L) represents the total length of a fake tree that originated with length value K. Wehave:

$$f(L) = P_f \times f(L-1) + f(L-1) + 1 \qquad ..3$$

Solving this recursive equation, we get

$$f(L) = \sum_{i=0}^{L-1} (P_f + 1)^i$$

$$= \begin{cases} \frac{(P_f+1)^L - 1}{P_f} & if P_f > 0 \\ L & otherwise \end{cases} \qquad ...4$$

Suppose the length of real path from the aggregator node to the base station is n. The cost is

$$C = \frac{M`}{M} = \frac{n + n \times P_f \times f(L)}{n} \qquad ..5$$

Hence,

$$C = \frac{n + n \times P_f \times \frac{(P_f+1)^L - 1}{P_f}}{n}$$

$$= (P_f + 1)^L \qquad ..6$$

If we combine Random walk and the residual energy based fake packet generation methods, the total cost is:

$$C = \frac{(P_f + 1)^L}{P_{er}} \qquad ..7$$

If we use fixed values of P_{er}, P_f and L , the average cost is a fixed value that is independent of the size of the network.

6 Problem Solutions

The simulations have been done in Castalia 3.2 [30]. Castalia is a simulator for Wireless Sensor Networks (WSN), Body Area Networks (BAN) and generally networks of low-power embedded devices. It is based on the OMNeT++ platform and can be used by researchers and developers who want to test their distributed algorithms and/or protocols in realistic wireless channel and radio models, with a realistic node behavior especially relating to access of the radio. Castalia can also be used to evaluate different platform characteristics for specific applications, since it is highly parametric, and can simulate a wide range of platforms. Castalia is based on OMNeT++ basic modules.

A simple module is the basic unit of execution. It accepts messages from other modules or itself, and according to the message, it executes a piece of code. The code can keep state that is altered when messages are received and can send (or schedule) new messages. There are also composite modules.

A composite module is just a construction of simple and/or other composite modules. The nodes do not connect to each other directly but through the wireless channel module(s). The arrows signify message passing from one module to another. When a node has a packet to send this goes to the wireless channel which then decides which nodes should receive the packet.

The nodes are also linked through the physical processes that they monitor. For every physical process there is one module which holds the "truth" on the quantity the physical process is representing. The nodes sample the physical process in space and time (by sending a message to the corresponding module) to get their sensor readings. There can be multiple physical processes, representing the multiple sensing devices (multiple sensing modalities) that a node has.

The node module is a composite one; most of the modules call a function of the resource manager to signal that energy has been consumed. The Application module is the one that the user most commonly change, usually by creating a new module to implement a new algorithm.

Castalia offers support for building our own protocols, or applications by defining appropriate abstract classes. All existing modules are highly tunable by many parameters. This is an effort to make the anti traffic analysis privacy preservation in wireless sensor networks energy efficient and thus leading towards the network lifetime optimization.

Table 1 Simulation parameters

Number of nodes	15
Simulation Time	100s
Node Deployment	Randomized_3x3
Mac Protocol Used	TMAC
Routing	Multipath Rings Routing
SN.field_x	30

SN.field_y	30
SN.wirelessChannel. Bidirectional.Sigma	0
SN.wirelessChannel.sigma	0
SN.node[*].Communication.Radio.TxOutputPower	-5dBm

The algorithm used is that there is a startup function that initializes all the values and variables on the sensor nodes. It checks whether it is an event generating node or not. If it is an event generating node then it sets a timer with send_packet a s an index and it is of 10 sec and for other nodes we set a different timer.

When this timer expires then this event generating node goes into a case of send_packet. There it tells every node that it is going to generate a packet and then it sends the data packet called as true_packet to the destination node. For every node when the timer expires it calculates its sensor reading for getting the remaining energy.

The introduced architecture of the simulated framework operation we added an additional mechanism that is based on residual energy of the node and average energy of the neighbor nodes. The node should generate fake packet on the basis of residual energy so that there is a balance between the node energy and additional traffic induced.

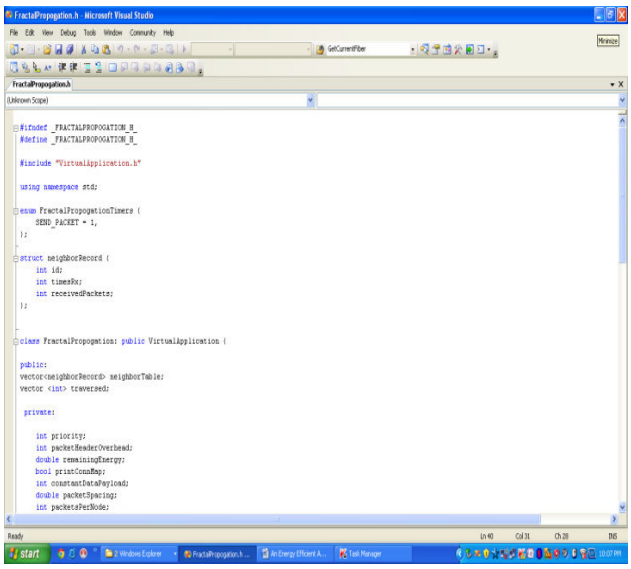

Fig.1. Snapshot of the simulated framework

This energy is read by the resource manager of the Castalia module and it gives back the energy of a sensor node, if this energy is greater than a threshold value then only a node will generate a fake packet.

Adding this residual energy constraint won't impose an overhead on the nodes which have low energy and thus they can they won't die early. When a node gets a packet it checks whether that packet is intended for it, if it is intended for it then it checks which packet it received that it is a true packet, fake packet or an event generating packet. If it is a true packet then it is forwarded to the intended node. If it is a fake packet then it is dropped and an event generating packet and a new fake packet is broadcasted to every node.

This ensures that traffic is uniform at every node and the privacy of the source location is preserved as the adversary cannot know from where the event generated just by analyzing the traffic. To make matters worse for an adversary, we can generate local high data sending rate areas, called hot spots, in the network. An adversary may be trapped in those areas and not be able to determine the correct path to the base station [31]. The set of techniques based on fractal propagation address both rate monitoring and time correlation attacks.

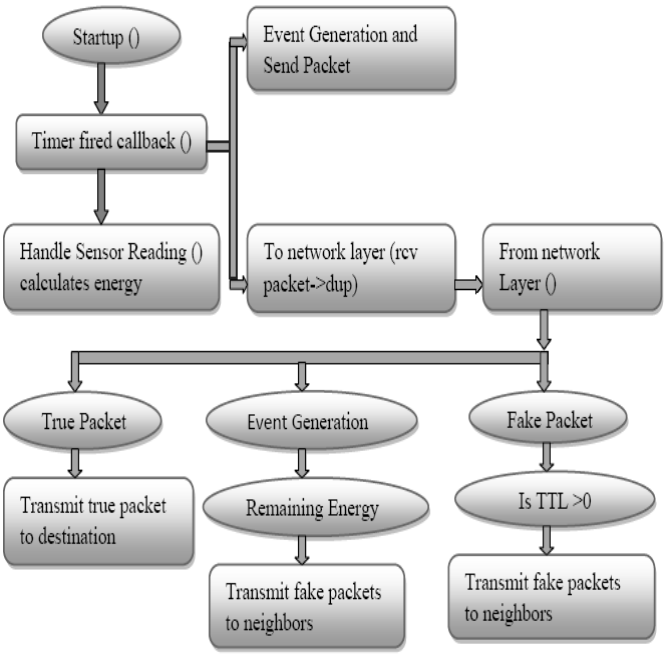

Fig.2. Flowchartof the simulated framework

A longer length of fake path will make it more difficult to launch a time correlation attack. Since a large fraction of packets are destined for the base Station, the sudden lack of forwarding is a strong indication that the base station area has been reached, even if we imposed a uniform sending rate on all nodes [32].

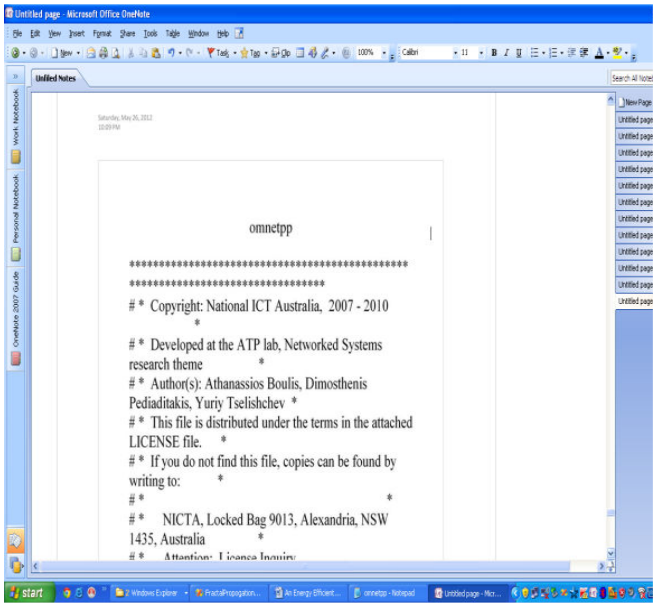

Fig.3. Snapshotof the output generating interface of the simulated framework

We have considered a technique whereby a base station that has received a packet continues to forward a dummy version of that packet past the base station.

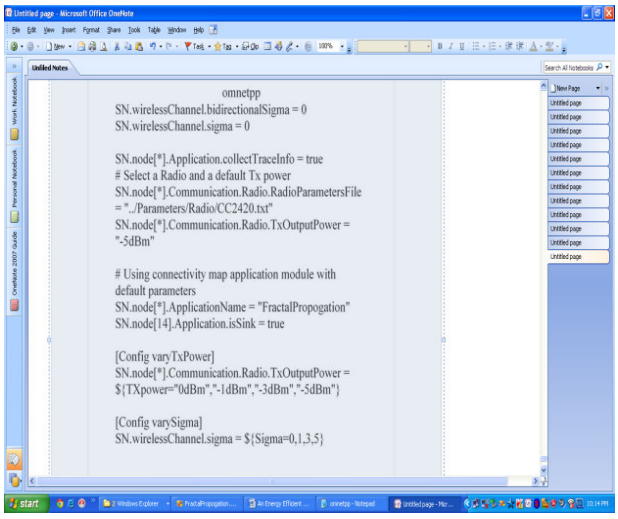

Fig.4. Snapshotof the output of the simulated framework

7 Results and Analysis

The results for energy consumption at each node for different simulated network of 100 seconds, 200 seconds and 300 seconds respectively present a less increase of energy consumption with the increase in network lifetime when the probability of fake packet generation was based on the residual energy based scheme as compared to the fake packet generation based on predefined probability.

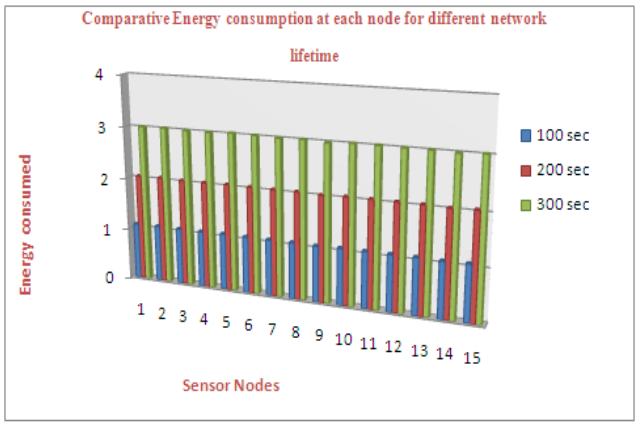

Fig.5. Energy consumption results at each node for different network lifetime

This may hence result in the improvement of the network lifetime as a whole. Though, the qualitative and quantitative privacy preservation of the current scheme has still to be verified. The energy consumption patterns for each node with the implementation of the residual energy based scheme for fake packet generation with different TTL values for fake packets 4 and 8 also present interesting results with a steep decrease in the energy consumption at each node as we decrease the TTL value from 8 to 4, with a very low decrease in the uniformity of traffic in the network.

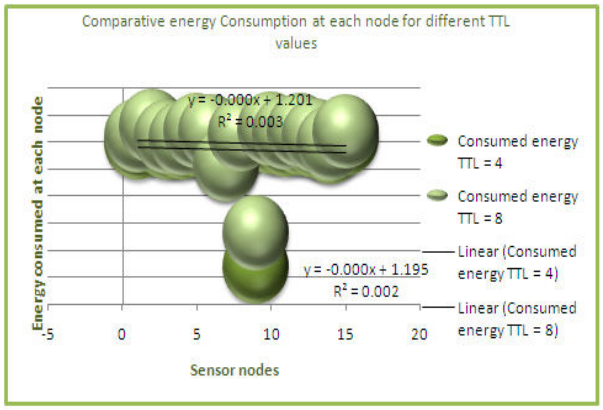

Fig.6. Comparative Energy Consumption at each node for different TTL values

Figure 7 presents the results for total transmitted packets (true packets+ fake packets) in the network. The total packets transmitted in the network without the implementation of residual energy based scheme of fake packet generation have been taken to be approximately same for both the simulation runs. Series 1 presents the total number of transmitted packets with the implementation of residual energy

based fake packet generation and TTL as 8 while series2 presents the results for total number of transmitted packets with TTL as 4.As it is evident by the results the scheme improves the network energy consumption by decreasing the total number of fake packets generated and transmitted in the network still maintain the traffic uniformity in the network.

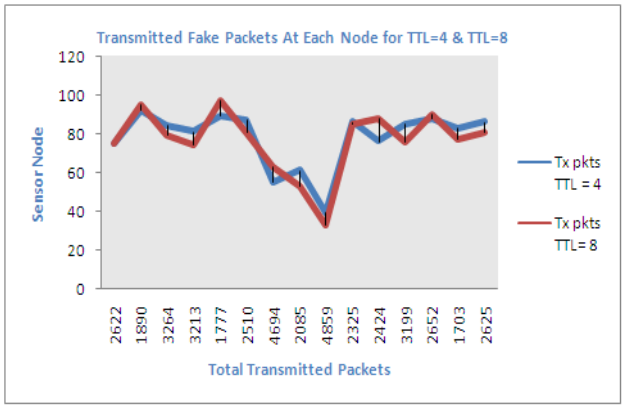

Fig.7. Comparative transmitted packets at each node for different TTL values and without any TTL.

8 Conclusions

The routing structure of a wireless sensor network is tree-based that is rooted at the base station [33]. Thusthe message transmission patterns are highly pronounced in and around the base station. This leads to revelation of location of the base station through traffic volume and directions of messages transmissions. This may prove to be a boon to the adversarymaking it capable of rate monitoring and traffic analysis attacks to locate and destroy the base station that is the central computational point of the entire WSN. The present paper proposed a residual energy based privacy provisioning for WSN .With the aim to countermeasures correlating network traffic to preserve location privacy of a base station that can be revealed in traffic analysis techniques [34]. We introduced residual energy based random fake paths taken by fake packets to confuse an adversary from tracking a message though certain amount of delay is added up to the transmitted packet to a base station. The simulations presented results supporting the proposed residual energy based fake packet generation scheme. The scheme achieved deco-relation comparable to the best possible deco- relation represented by the broadcast, at a fraction of broadcast's messaging cost.

Also these fake packets have a limited lifetime with the TTL value so as to optimize the energy consumption overhead in the network. The idea of fake packet propagation aids significantly in spreading out the communication traffic evenly over the network and obfuscating any paths to the base station with a little delay that too may be utilized for temporal privacy preservation.

9 Future Perspectives

The future prospective for the current research induces the key idea to generate hotspots in the network to trap the adversary [35]. To enhance the deco relation in traffic further local high data sending rate areas are generate, called hot spots, in the network. An adversary may be trapped in those areas and not be able to determine the correct path to the base station. The challenge here is how to create hot spots that are evenly spread out in the network, such that only a minimum (preferably zero) amount of extra communication/coordination among the sensor nodes is needed.

This may be done by letting the nodes that forwarded fake packets earlier have a higher chance to forward fake packets in the future. This way, after a node has forwarded a fake packet to one of its neighboring nodes, it will continue to forward other fake packets to the same neighboring node with higher and higher probability. If an area of nodes receive fake packets, they are more likely to process more and more fake packets in the future. This will turn that area into a hot spot. It is also very easy to destroy current hot spots and reconstruct new hot spots at different places. For example, sensor nodes just reset the value of tickets to 1 when they receive a broadcast message from the base station, and then start to build hot spots from scratch.

A patient attacker can wait at a hot spot until the communication pattern changes. While this will allow the attacker to determine that he was at a fake hot spot, it does not provide any other information about the possible location of the base station. Furthermore, waiting for a long time at a fake hot spot will add more delay to finding the location of the base station.

References:

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci.A survey on Sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[2] Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham , "Privacy preservation in wireless sensor networks: A state-of-the-art

survey" in Ad Hoc Networks 7 (2009), p. 1501–1514, 2009.

[3] J. Deng, R. Han, and S. Mishra. Security, privacy, and fault tolerance in wireless sensor networks. Artech House, August 2005.

[4] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, September 2003.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc, 2005.

[6] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In ACM WiSe, pages 80–89, 2004.

[7] G. Gaubatz, J.P. Kaps, and B. Sunar. Public key cryptography in sensor networks - revisited. In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.

[8] J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pages 43–52, New York, NY, USA, 2004. ACM Press.

[9] R. Zhang, Y Zhang, and K. Ren,"DP 000b2;ac: Distributed privacy preserving access control in sensor networks", in INFOCOM 2009, IEEE, pp. 1251-1259, April 2009

[10] Perrig et. al. SPINS: Security Protocols for Sensor Networks. Wireless Networks, 8(5):521–534, 2002.

[11] Aysal, T.C.; Barner, K.E.; Sensor Data Cryptography in Wireless Sensor Networks. In IEEE Transactions on Information Forensics and Security, Volume: 3 Issue:2
On page(s): 273 – 289,2008

[12] R. Zhang, Y. Zhang, K. Ren, "DP2AC: Distributed privacy-preserving access control in sensor networks", in proceedings of the 28th IEEE International Conference on Computer Communications (INFOCOM 2009), pp.1298–1306, 2009.

[13] Pandurang Kamat, Wenyuan Xu, Wade Trappe, Yanyong Zhang , "Temporal Privacy in Wireless Sensor Networks" in International Conference on Distributed Computing Systems, 2007, ICDCS'07, p. 23-35,27 june 2007.

[14] A. Cerpa and D. Estrin, "ASCENT: Adaptive Self-Configuring Sensor Networks Topologies," in Proceedings of IEEE INFOCOM'02, June2002.

[15] Jing Deng, Richard Han, Shivakant Mishra, "Decorrelating Wireless Sensor Network Traffic To Inhibit Traffic Analysis Attacks" in Elsevier Pervasive and Mobile Computing Journal, Special Issue on Security in Wireless Mobile Computing Systems, vol 2, issue 2, pp. 159-186, April 2006.

[16] W.S. Zhang, C. Wang, T.M. Feng, "GP^2S: generic privacy-preservation solutions for approximate aggregation of sensor data", in proceedings of the Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), Hong Kong, P.R.C., pp.179–184,March 17–21, 2008.

[17] C.Ozturk, Y. Zhang, and W. Trappe. "Source-location privacy in energy-constrained sensor network routing". In SASN'04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004.

[18] Yi Ouyang, Zhengyi Le, Yurong Xu, N. Triandopoulos, Sheng Zhang,J. Ford, and F. Makedon. Providing anonymity in wireless sensor networks. In Pervasive Services, IEEE International Conference on, pages145-148, July 2007.

[19] Yong Xi, L. Schwiebert, and Weisong Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In IEEE International Parallel and Distributed Processing Symposium, Los Alamitos, CA, USA, 2006. IEEE Computer Society.

[20] Jing Deng, Richard Han, and Shivakant Mishra. Intrusion toleranceand anti-traffic analysis strategies for wireless sensor networks. In DSN'04: Proceedings of the 2004 International Conference on Dependable Systems and Networks, pages 637-646, Washington, DC, USA, 2004 IEEE Computer Society.

[21] Celal Ozturk, Yanyong Zhang, and Wade Trappe. Source-location privacy in energy-constrained sensor network routing. In SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor

networks, pages 88-93, New York, NY, USA, 2004. ACM.

[22] Jing Deng, Richard Han, and Shivakant Mishra. Countermeasures against traffic analysis attacks in wireless sensor networks. In SECURECOMM '05: Proceedings of the First International Conferenceon Security and Privacy for Emerging Areas in Communications Networks, pages 113-126, Washington, DC, USA, 2005. IEEE Computer Society.

[23] Yong Xi, L. Schwiebert, and Weisong Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In IEEE International Parallel and Distributed Processing Symposium, Los Alamitos,CA, USA, 2006. IEEE Computer Society

[24] P.F. Syverson, D.M. Goldschlag, and M.G. Reed. Anonymous connections and onion routing. In Proceedings of IEEE Symposium on Security and Privacy, 1997, pages 44-54, May 1997.

[25] Y. Xi, L. Schwiebert, W.S. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks", in: Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), April 2006.

[26] Xiaoyan Hong, Pu Wang, Jiejun Kong, Qunwei Zheng, and jun Liu. Elective probabilistic approach protecting sensor traffic. In Military Communications Conference, 2005. MILCOM 2005. IEEE, volume 1,pages 169-175, Oct. 2005.

[27] Jing Deng, Richard Han and Shivakant Mishra : Defending Against Traffic Analysis Attacks in Wireless SensoNetworks.www.usenix.org/event/sec04/tech/wips/posters/05-deng-wireless.pdf

[28] J. Luo, and J.- P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks", Proceedings IEEE INFOCOM'05, vol. 3, Miami, FL, Mar. 2005, pp. 1735-1746.

[29] Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks", in the Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, San Francisco CA, April 2001, pp. 2009-1015.

[30] http://castalia.npc.nicta.com.au/

[31] Y. Jian, S.G. Chen, Z. Zhang, L. Zhang, "Protecting receiver-location privacy in wireless sensor networks", in proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007), pp. 1955–1963, May 2007.

[32] Z. Cheng and W. Heinzelman, "Flooding Strategy for Target Discovery in Wireless Networks," in proceedings of the Sixth ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2003), 2003.

[33] Haodong Wang, Bo Sheng, and Qun Li. Privacy-aware routing in sensor networks. Computer Networks,

[34] P. kamat, Y. Zhang, W trappe, and C. Ozturk,. Enhancing source-location privacy in sensor network routing. in Proceedings. 25th IEEE International Conference on Distributed Computing Systems, 2005.ICDCS 2005, pp. 599-608, june 2005.

[35] R.A. Shaikh, H. Jameel, B.J. d'Auriol, Sungyoung Lee, Young-Jae Song,and Heejo Lee. Network Level Privacy for Wireless Sensor Networks. InFourth International Conference on Information Assurance and Security, 2008, pages 261-266, Sept. 2008.

BIOGRAPHIES

Ms. Manjusha Pandey is pursuing her Ph.D. from Indian Institute of Information Technology, Allahabad, India in Information and Technology, has done her M. Tech in Computer Science.

Her research interest areas include Wireless Sensor Networks, Privacy in Wireless Communication, Privacy and security in Digital & Mobile Communication, Signal Processing and Vehicular Technology.

Dr. Shekhar Verma Received his Ph.D. degree from I University, Varanasi, India in Computer Science and Engg. He is Associate Professor in Information Technology at

Indian Institute of Information Technology, Allahabad, India. His research interest areas are Computer Networks, Wireless Sensor Networks, Vehicular Technology, Cryptography, Information and Network Security.