I. J. Computer Network and Information Security, **2012, 4, 21-29**
Published Online May 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.04.03

Residual Energy Based Anti-Traffic Analysis Privacy Preservation in WSN

Manjusha Pandey , Shekhar Verma
Indian Institute of Information Technology, Allahabad, India.
rs58@iiita.ac.in, sverma@iiita.ac.in

Abstract— Present paper is an effort to build an energy efficient mechanism which can preserve the privacy of the location of base station and the source nodes so that the adversary cannot take down these nodes. Core functionality of WSN includes routing of the sensed data through predetermined optimized routes to the base station thus producing pronounced traffic near the sink node adding up to the revelation of either location of direction of location of base station. To overcome this revelation of base station the traffic patterns may be disguised by introducing fake packets to the generated traffic of original data. Many anti traffic analysis strategies have been proposed and implements with the objective of attaining traffic uniformity in network. But the inclusion of fake packets adds up communication overhead 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.

Index Terms— Wireless sensor networks, Privacy in WSN, Traffic analysis, energy efficiency, communication patterns, energy efficiency, network lifetime

I. 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.

Present day sensor nodes are much more advanced than their predecessors owing to the advances in nano technology and fabrication techniques, and these improved sensor nodes have enhanced the potential application domain of sensor networks providing ability to observe the previously unobservable physical space at a finer resolution over large spatio-temporal scales. Advances in sensor technology have also amounted to the betterment of in network processing done by these tiny devices like data fusion and correlation along with data communication. The routes followed by data in sensor networks are dependent on the application and is implemented by the corresponding nodes through neighbor discovery that perform a distributed algorithm to route the data within the network. Sensor networks discover and adapt connectivity prior because along with the physical placement of node various other factors like obstructions, interference, environmental factors, antenna orientation and node mobility are also responsible for variations in connectivity of the nodes [2, 3].These remarkable characteristics of WSN make security and privacy in these networks peculiar. Also the sensor nodes are non immune to physical capture because of their low cost and tamper resistant hardware making the whole network and wireless communication among nodes vulnerable to eavesdropping[4]. To drain out the battery power of sensor nodes an attacker may flood the network with malicious messages as the network is a resource constraint network having complex design issues. Advanced anti-jamming techniques like frequency hopping and spread spectrum could not be used in sensor networks and make the network more susceptible to denial of service attack [6].The adversary may use various link attacks like passive eavesdropping or active interfering leading to leakage of secret information or node impersonation. Large scale deployment of sensor networks generates the need for scaling of various cryptographic alternatives proposed and implemented for security and privacy preservation [7]. Many of the security schemes in WSN use symmetric key cryptography as centralized keying is not possible due to small memory capacity and energy constraint of WSN. Thus WSN poses a contradictory interest of minimizing the resource consumption along with enhanced security and privacy preservation with the aim that a better solution must provide a good compromise between the two.

II. Issues and Challenges

In the field of wireless sensor networks various researchers have been done to counter the distinct and challenging characteristics of its behavior, mainly in the domain of MAC, Routing, Time synchronization, Data Aggregation[12] etc. In spite of the importance of time and spatially important data, providing privacy has not been much researched domain. Ensuring privacy is not at all a less important objective in comparison to other domains in sensor networks, because gathered are critical both in term of its time and spatial significance such as;

volcano monitoring, earthquake Monitoring etc. Providing privacy to the data gatherers, Transmitted and processed at sensor nodes is an important task.

Privacy is not only crucial in terms of content of data; it's also significant with respect to the context of data. Context of data can be visualized as the source of data, event originating in the network, timestamp of data gathered etc [13]. For example in habitat monitoring applications, data regarding movement patterns of the animals can deter the objective of the applications. Several potential challenges in sensor network hamper the assurance of privacy. Some of these challenges are described below:

a) Ungovernable environment: The sensors can be placed in a intimidating place where the adversary can place counterfeit sensors. Such applications can be like warfare field surveillance. The adversary can also physically damage the sensor node itself. Either way it violates the integrity of the network, and an adversary can gain access to the private keys.
b) Resource constraints: The sensors are low on battery power and storage so we cannot use conventional cryptographic mechanisms for privacy preservation in sensor networks as they have high complexity and the public key ciphers consume resource intensively.
c) Constraints on Topology: As the sensor nodes are multi-hop networks. In these the nodes that are in the near of the base station relay the traffic of the sensor nodes and also its own data so an adversary which can investigate the traffic and can get the place of the sink node [14].

III. Problem definition

A major threat to the location privacy of base station is pronounced traffic patterns towards the base station as the nodes near the base station forward larger volume of data as compared to other nodes in the network. Traffic analysis helps the adversary to deduce the location of base station and topology of sensor network which along with the knowledge of routing parameters may pose a serious threat to privacy attacks for the base station. The present research work proposes energy efficient anti traffic analysis privacy preservation mechanism against this type of traffic analysis tacks in WSN.The aim is to restrict the adversary from analyzing packet transmission within the area of its presence which may further help it to analyze the flow of traffic towards base station.

The overall objective is to have a uniform traffic within the network. In particular, our goals are:

- Analysis of event generation and statistical flow of data transmission must not help the adversary in deduction of data flow direction.
- Statistical analysis of packet transmission rate should not reveal the data transmission direction

The most primitive form of defense is to encrypt each transmitted packet but this requires hop by hop encryption as the adversary may follow encrypted packet transmission pattern towards its destination that is base station. To defeat this each packet may be re encrypted at each hop with pair wise key schemes but still the adversary is able to deduce significant information by monitoring traffic volume or time correlation. The act of transmitting itself reveals information to the attacker, regardless of whether packet contents can be inspected.

IV. Related Work

Based Privacy preservation in senor network differ a lot from the traditional networks as the senor 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 senor 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 level value 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 level value 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.

V. Residual Energy Based Fake Packet Generation & Recommendations

Privacy preservation of location of sensor nodes as well as the base station in wireless sensor networks by concealing traffic dynamics has been achieved through various mechanisms as discussed in section IV but there are pros and cons of all the mechanisms and one of the major drawbacks of all the proposed mechanisms is energy overhead introduced by these mechanisms. Hence we propose a residual energy based fake packet generation scheme as advancement over the earlier proposed fractal propagation. In fractal propagation several fake packets are created and propagated within the network in order to make the traffic patterns more more random. A node generates and propagates fake packets with a fixed probability to its neighboring nodes as soon as it hears any of its neighboring nodes propagating the real data packet. The transmission path of these fake packets spread out in network and form a tree .Hence the communication traffic is much more spread out than the earlier techniques of random walk and this restricts the adversary from tracking the real packet even if she track using time correlation. But creation of fake packets by all neighboring nodes with a constant probability takes a toll on energy consumption and network lifetime [27] .

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. 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 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 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].

Algorithm1: Calculation of Mean Energy Probability for Fake Packet Generation

Step1: Initialization

Step2: If $E_{avg} = E_r$

Then $P_{er} = P_t$

Step3: Else if $(E_r > E_{avg})$

Then $P_{er} = P_{Max}$

Else

$P_{er} = P_{Min}$

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.

MAXIMUM AND MINIMUM PROBABILITY FOR FAKE PACKET GENERATION

$$P_{Max} = \frac{P_t + (1.0 - P_t) * (E_r - E_{avg})}{(E_{max} - E_{avg})}$$

$$P_{Min} = P_t * \frac{Er}{Eavg}$$

Where
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 neighbor
P_t = threshold probability set to some predefined value (0.6, 0.2, 0.4)
P_{Max} = Maximum forwarding probability
P_{Min} = Minimum forwarding probability
P_{er} = Fake packet forwarding probability

We have

$$f(L) = P_f \times f(L-1) + f(L-1) + 1 \quad (1)$$

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.

ALGORITHM 2 CALCULATION OF AVERAGE ENERGY OF NEIGHBORS

Step1: Initialization
$E_{avg} = E_r$

Step2: Node sends beacon to its neighbors
Step3: Reply (E_{avg}) to node N_x
Step4: Calculate $new\ E_{avg} = average$ (Rx (E_{avg}),E_r)
Step5: $E_{avg} = new\ E_{avg}$

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.

We have

$$f(L) = P_f \times f(L-1) + f(L-1) + 1 \quad (1)$$

Solving this recursive equation, we get

$$f(L) = \sum_{i=0}^{L-1} (P_f + 1)^i = \begin{cases} \frac{(P_f+1)^L - 1}{P_f} & if P_f > 0 \\ L & otherwise \end{cases} \quad (2)$$

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

$$C = \frac{M`}{M} = \frac{n + n \times P_f \times f(L)}{n} \quad (3)$$

Hence,

$$C = \frac{n + n \times P_f \times \frac{(P_f+1)^L - 1}{P_f}}{n} = (P_f + 1)^L \quad (4)$$

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

$$C = \frac{(P_f + 1)^L}{P_{er}} \quad (5)$$

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.

VI. SIMULATION SETUP

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.

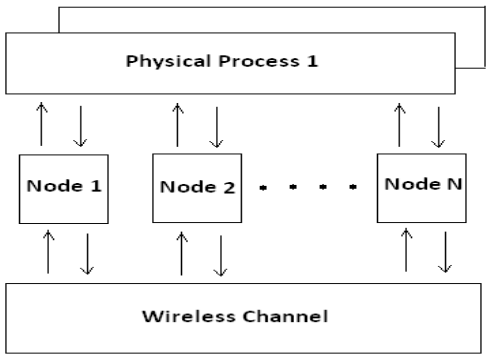

Figure 1. Layered representation of simulated framework operation

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. Figure 1 shows the internal structure of the node composite module. The solid arrows signify message passing and the dashed arrows signify simple function calling. For instance, 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. The following figure 2 presents node module of the simulated framework operation for the residual energy based fake packet generation. 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.

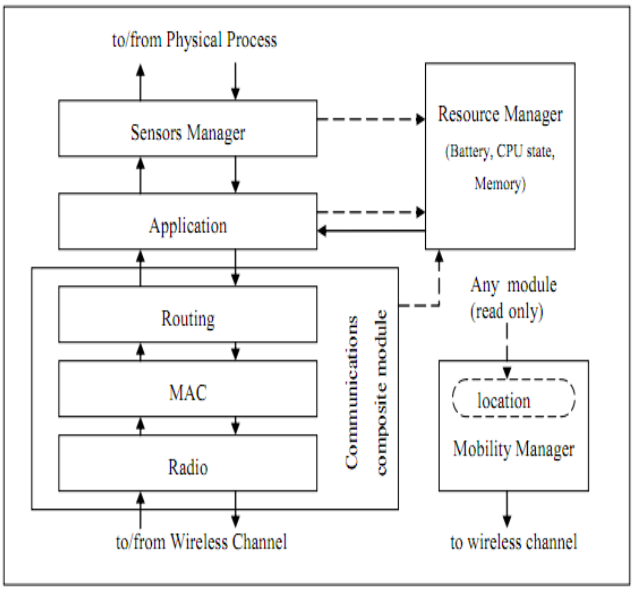

Figure 2 Node module of the simulated framework operation

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.

In the present 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. 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.

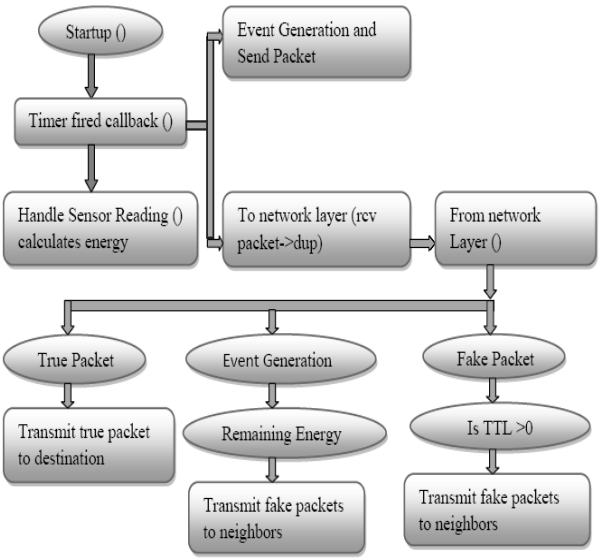

Figure 3 Architecture of the simulated framework operation

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.

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]. I 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.

VII. Results and Analysis

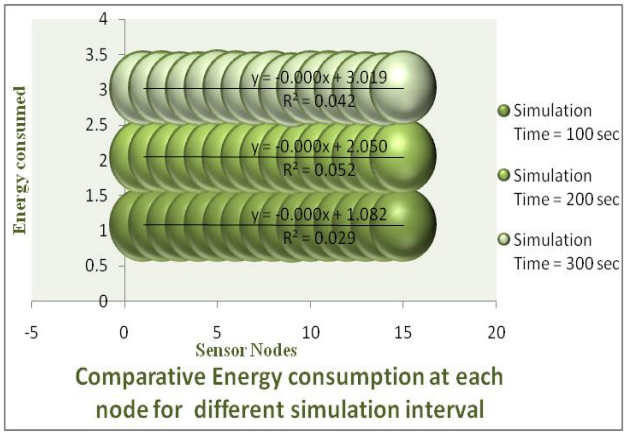

Figure 4 Energy consumption results at each node for different simulation intervals

The results for energy consumption at each node for different simulation intervals of 100 seconds, 200 seconds and 300 seconds respectively present a less increase of energy consumption with the increase in simulation time 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. 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.

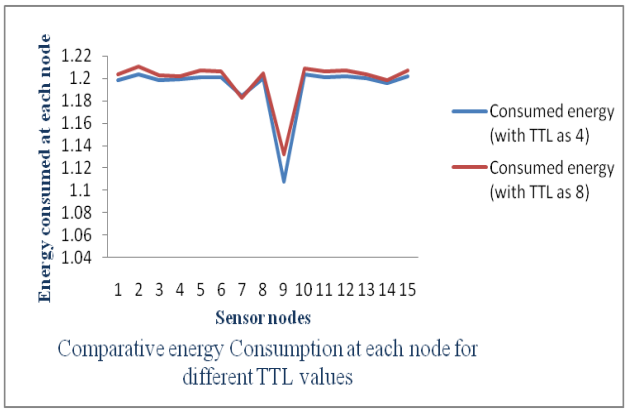

Figure 5 Comparative Energy Consumption at each node for different TTL values

Figure 6 presents the results for total transmitted packets (true packets+ fake packets) in the network. Series1 depicts the total packets transmitted in the network without the implementation of residual energy based scheme of fake packet generation. Series 2 presents the total number of transmitted packets with the implementation of residual energy based fake packet generation and TTL as 8 while series3 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.

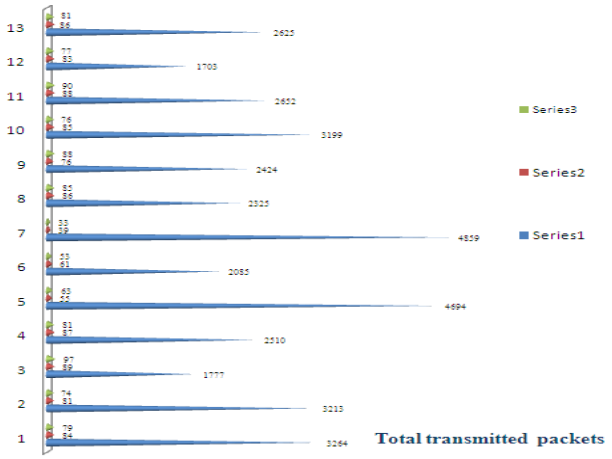

Figure 6 Comparative transmitted packets at each node for different TTL values and without any TTL.

VIII. Conclusion

The tree-based routing structure of a wireless sensor network is rooted in a base station [33]. The forwarding patterns of WSNs are highly pronounced, revealing the location of the base station through traffic volume and directionality of packet forwarding. An adversary can eavesdrop and employ rate monitoring traffic analysis attacks to locate and destroy a base station, thus disabling the entire WSN. The present paper proposed a residual energy based countermeasures aimed at decor relating network traffic so that the location of a base station is disguised against traffic analysis techniques [34]. We introduced residual energy based random fake paths taken by fake packets to confuse an adversary from tracking a packet as it is transmitted to a base station. The simulations showed that our residual energy based fake packet generation scheme, achieved deco-relation comparable to the best possible deco- relation represented by broadcast, at a fraction of broadcast's messaging cost.

The residual energy based propagation approach makes it more difficult to trace a packet by inspecting transmission times of adjacent nodes, because the attacker may wind up following a path followed by fake packet to a dead end.

Also these fake packets have a limited lifetime with the TTL value so and can be stopped forwarding by following nodes. 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. To make matters worse for an adversary, we can also 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. 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.

IX. Future Perspective

The future prospective for the current research induces the key idea to generate hotspots in the network to trap the adversary [35]. 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] A. 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, "DP^{2}AC: 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] A. 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.

Manjusha Pandey is pursuing 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.

Shekhar Verma received his Ph.D. degree from IT, Banaras Hindu 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.

