Toward Secure Data Sharing Protocols for Avoiding Global Eavesdropper in WSN

G. Arock Nancy[1] , V.Hamsadhwani[2]
[1]M.Tech Scholar, Department of Information Technology,
Periyar Maniammai University, Thanjavur, Tamil Nadu, India
[2]Assistant Professor, Department of Information Technology,
Periyar Maniammai University, Thanjavur, Tamil Nadu, India
[1]arocknancy@gmail.com
[2]bellhwk@yahoo.co.in

***Abstract*— While transformation of the data between communications system there is need for confidentiality of content and location. In existing work only capable of preserving the content and protection on a limited portion of the network at a time. This paper focuses on provision of protecting location against a global eavesdropper. Mobility prediction algorithm is the proposed technique which is implemented for preserving the location of nodes. It provides the confidentiality of the location in wireless sensor. Performance evaluation shows that our proposed method outperforms the existing method.**

Keyword—Sensor, Mobility prediction, Global Eavesdropper

I. INTRODUCTION

Networks are both wired and wireless. There is not possible to monitor or control the entire network by a single node. There is a need to setup [5] each node with of administrator. Wireless Sensor network (WSN) has generated tremendous interest among researchers these years because of their potential usage in a wide variety of applications**.** Data sharing in wireless sensor network includes the following components. Figure 1 shows the components of WSN.

- ***Sensor Field*:** Sensor field include sensor nodes. In the sensor field sensor nodes are communicate with each other.
- ***Sensor Node*:** In includes communication nodes. Data are transferred between these nodes.
- ***Gateway*:** A Gateway also known as access point, which enables the communication between sink and sensor nodes [14].
- ***Task Manager*:** Task manager involves with performing some actions.
- ***Network manager*:** Network manager [14] involves in the network activities like network configuration, scheduling, monitor and controls the network
- ***Security Manager*:** The Security manager involves in the network for the security purpose. it involves [14] generation, Storage, and management of keys.

Sensor nodes [1] can be used for event detection and location sensing. WSN mainly used for monitoring and recording any physical or environmental conditions. Sensor nodes collect data from the environment, locally process this data and transmit the sensed data back to the user. The target information are passed to the main location through network. Sensor networks are used in most applications [1] such as wildlife habitat monitoring, security and military surveillance, environment, health, home, other commercial areas and target tracking.

WSN applications can be classified into two categories: monitoring and tracking. Monitoring involves periodic data collection. When a certain event occurs in the sensing field, sensor nodes collect the sensor readings of that certain event and transmit them back to the sink. Tracking applications have different requirements than monitoring applications. This is because in target application the source of an event is a mobile node. Real-time communication is usually desired in tracking applications

Consider an example [2] of military surveillance. In this application sink may collect the information about enemy through sensors. A strong adversary tries to eavesdrop on network traffic by compromising the sensor nodes to obtain the valuable information. Misuse of such information by an adversary cause financial losses and affect human lives. So there is a need to increase some security services like confidentiality, authentication, and integrity.

Confidentiality of location is very important in wireless sensor network. This is because when the location is known by an adversary, they will easily hack the information. To avoid eavesdropper compromising the sensor node make stability path among the nodes.

Hence we proposed mobility prediction algorithm for preserving the contextual information. Mobility prediction can significantly improve routing and provide the confidentiality of the location, allows estimating the stability of paths in wireless sensor networks. The mobility prediction algorithm needs only to identify the next connection point of the mobile user with respect to the network.

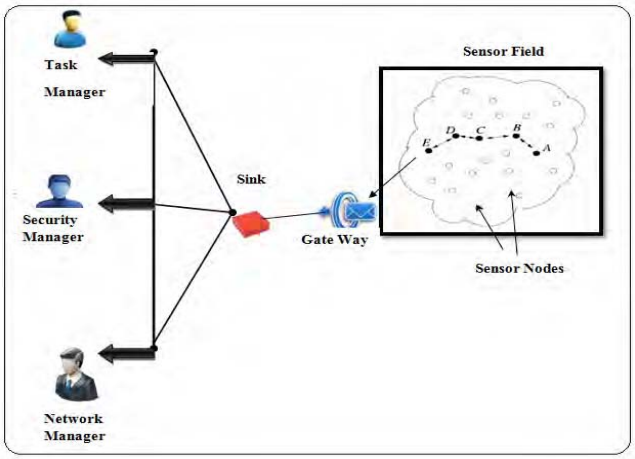

Fig.1.Components of WSN

The source and sink in wireless sensor network can be mobile, where the source and sink are free to connect to the network or disconnect at any time, it should have the capabilities of receiving traffic, easily attacked by an adversary.

Existing work guard only the content of the information from a limited adversary in a small region. This information can be hacked by global eaves dropper. At the same time, the Eavesdropper compromises the subset of sensor nodes. The drawback of this existing system are First adversary easily attack the network. Second Communication is expensive. Third it has limited processing speed. This paper focuses on provision of protecting location against a global eavesdropper. Mobility prediction algorithm is the proposed technique which is implemented for preserving the data.

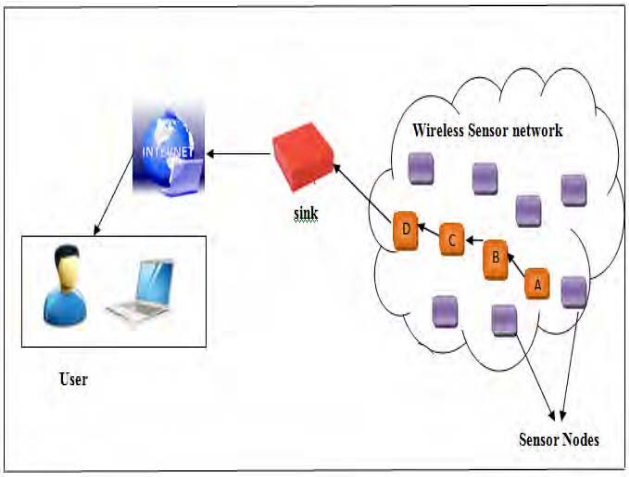

Fig.2. Data sharing in wireless sensor network

II. RELATED WORK

In recent years secure data sharing has been an interesting research area. While sharing data between communication nodes, user may want to retrieve location based data and content of the data without revealing their location. The adversary monitors the wireless transmissions to infer locations of critical infrastructure Existing technique has developed most secure sharing method. Those methods are limited with small region and local eavesdropper. In [6] the information is transferred by using routing protocol. Here to confuse the eavesdropper fake packets are injected through network traffic.

Fake packet generation creates fake sources whenever a sender notifies the sink that it has real data to send. The fake senders are away from the real source and approximately at the same distance from the sink as the real sender. The drawback of this method is the adversary may interfere in the network traffic is shown in figure 2. Another drawback is fake packets and original packets are distributed. The location can be preserved

by hiding the source location from eavesdropper. This is described in [8]. The problem in this technique is adversary may collect the information from sink.

In [11] [13] by observing the wireless signal from the user device user location privacy can be compromised. These compromising the sensor nodes by the eavesdropper problem are reduced by random delay and dummy traffic Phantom single-path routing [7] achieves location privacy by making every packet walk along a random path before being delivered to the sink. To provide privacy for content and originator and to reduce the energy consumption they described the flooding protocols [10].

The flooding technique has the source node send each packet through numerous paths to a sink, making it difficult for an adversary to trace the source. It does not provide privacy for base station and Low reliability. Thus to increase the network life time and save energy in wireless sensor network [3] propose backbone routing which consists of backbone nodes awake and transmit the packets, The Demerits in this paper is delay can be occurred. It does not work for network performance.

By creating the looping paths at various places in the network called cyclic entrapment [9]. It can fool the adversary. This can increase the safety period. All these techniques are developed for local eavesdropper who is only capable of eavesdropping on a small region. A global eavesdropper can easily overcome these techniques by locating the first node initiating the communication with the base station.

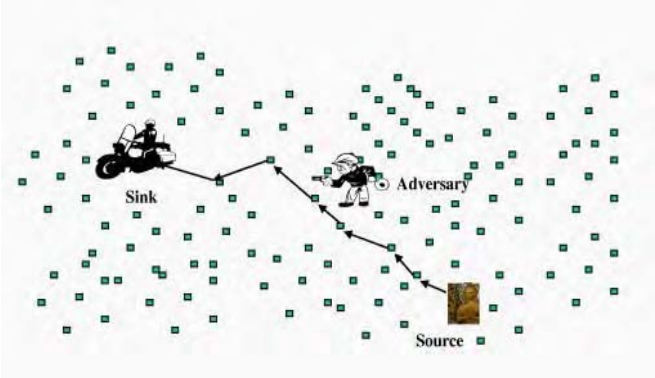

Fig.3.Adversary Eavesdropping

In [4] it was shown that an adversary can track sinks by carrying out time correlation and rate monitoring attacks. To mitigate these two kinds of attacks, Deng et al. introduced a multiple-parent routing scheme, a controlled random walk scheme, a random fake path scheme, and a hot spots scheme [4].However, these techniques all assume that the adversary is a local eavesdropper. A global eavesdropper can easily defeat these schemes. For example, the global eavesdropper only needs to identify the region exhibiting a high number of transmissions to locate the sink. This paper focus on providing confidentiality of the location designed to defend against a global eavesdropper using mobility prediction. Mobility prediction algorithms use a history base that has a record of the previous movements of nodes.

In [16] Mobility prediction allows estimating the stability of paths in a mobile wireless Ad Hoc networks. Identifying stable paths helps to improve routing by reducing the overhead and the number of connection interruptions. In [17] proposes an activity based mobility prediction technique that uses activity and Markov Modeling techniques to devise a prediction methodology that could make accurate predictions than existing techniques.

Yang et al. propose to use proxies to shape the network traffic such that global eavesdroppers cannot infer the locations of monitored objects [15]. This paper focuses on provision of protecting location against a global eavesdropper. Mobility prediction algorithm is the proposed technique which is implemented for preserving the location of nodes. This mobility prediction algorithm is used to identify the next connection point of the mobile user with respect to the network. It provides the confidentiality of the location in wireless sensor.

III. PROBLEM DEFINITION

Protocols used for exchanging information between communication nodes. When transferring information between nodes it brings only privacy for the content of the information. There is lacking of privacy in contextual information. The reason is such contextual information is used by an adversary, to derive sensitive information like locations of monitored objects and data sinks in the field. Existing work proposed the technique for small region and local eavesdropper. Mobility prediction algorithm is the proposed technique towards secure data sharing against global eavesdropper.

A. Context Definition

Three important aspects of context are: where your are, who you are with and whatresources are nearby. Context is any information that can be used to characterize the situation of an entity . In general Mobile peer-to-peer environment with limited resources forces to focus on certain context attributes. The context awareness is important for source and sink.then only they avoid hacking the information.

B. Context Awareness

- Gather knowledge of currently surrounding nodes
- Enable prediction of behavior of nodes
- Consider probability of failure of nodes

IV. SYSTEM MODEL

While transferring of information between communication nodes, the exchanging of information carried out by the intermediate nodes. Using Mobility prediction algorithm the node predicts the location of the neighbor nodes. Each sensor node has own id and it maintains energy level. Initially a sensor node sends a request to its neighbor node. The neighbor node sends the acknowledgement. This information is maintained by the mobility prediction module. Every node checks its neighbor node location, id and energy level. Based on the energy level the sensor node accepts the requests from the neighbor node otherwise it assumes that it is eavesdropper node. So it rejects the communication.

Mobility prediction means estimation of their future locations of the nodes. The location definition differs for various networks: In infrastructure networks, location means the access point to which the node is connected. The main advantage of mobility prediction is before the mobile node leaves, the next location is predicted. It is used to avoid the interruption time between communication nodes. In networks without infrastructure or MANETs, location defines the geographic coordinates. There are two different methods for mobility prediction. According to these methods the node moving is calculated by RWM (Random Waypoint Mobility) model. When nodes are moving using such methods it can lose its accuracy and efficiency. It can be overcome by wireless sensor network

In this paper, assume that each node in the wireless sensor network is aware of its location. GPS (Global Positioning System) is used for learning location. The advantage of this GPS system is it can periodically record the geographical location. Figure 4 shows the node mobility path. The mobility time is denoted by Δ_m.

The path is noted as: ($X\Delta_m$, $Y\Delta_m$, $Z\Delta_m$). The previous locations are denoted by ($X\Delta_{m-1}$, $Y\Delta_{m-1}$, $Z\Delta_{m-1}$). The estimated future location is denoted as ($X\Delta_{m+}1$, $Y\Delta_{m+1}$, $Z\Delta_{m+1}$)

The merits of mobility prediction algorithm are

- Future locations prediction
- Ensuring the availability of the network services anywhere and anytime
- Successful handoffs are possible
- QoS –dropping rate and new connection blocking rate

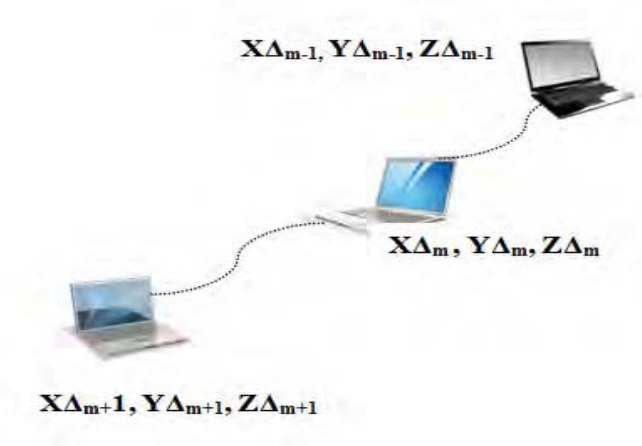

Fig.4.Mobility prediction

A. Flow Diagram

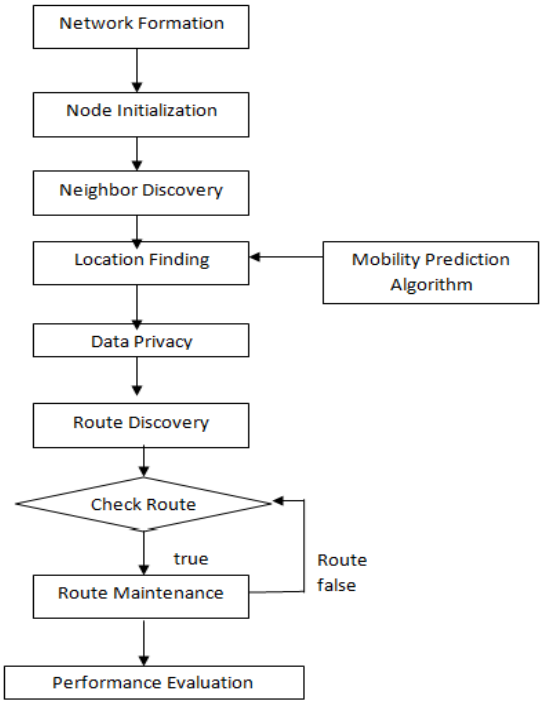

Fig.5. Flow Diagram

Figure 5 shows the flow diagram for the system. Initially the network has formed as globally. Then node has created as per the network need. Each node participates to discover the neighbor. Location finding is carried out by the mobility prediction algorithm. Privacy mechanism is used for secure transmission of data. Find the route to where the data is send from the source. For each transmission of data, the network has checked whether the route is correct or not. The performance evaluation carried out using simulation tool in this paper.

V. OVERVIEW OF PROPOSED SYSTEM

A. Description

Mobility prediction algorithm defines the estimation of the future location of the communication nodes in the wireless sensor network.

B. Algorithm Definition

Initially the nodes start to communicate with its neighbor nodes in the region. To discover the neighbors, each node sends the beacon messages to it neighbor nodes. Beacon packets contain all the information about network. After each node knows about its neighbors, Source and Sink start to communicate with each other. Source will decide the path through which the data are transmitted. Initially source node defines the current location as $\Delta_{curr.}$

Then these nodes finds, which current location is minimum, it is denoted by $\Delta_{min.}$ The node starts action for scheduling, and all the scheduling is stored in mobility prediction table called mobility prediction module. The node calculates its future location based on minimum current location, current action, random conditions and traces. During each action the nodes movement is informed to the mobility module. Each node transfers the information to the sink based on minimum current location.

Pseudo code

Input : Current Location L_c

Output: Predicted Location L_p

1: $L_p = 0$; for Initial node

2: // initially set predicted location is empty

3: for each { $L_c = L_{c1} + L_{c2} + + \ldots\ldots\ldots + L_m$ }

4: m: maximum distance path; $L_p < L_m$

5: L_{C1} = Update (L)

6: Wait for Initial Update

7: L_{C2} = Update (L_{C1})

8: Calculate V

9: V ← Neighbor node

10: $Node^+ = V + L_c$

11: // Generate Node by attaching V to the L_c

12: ? = $Node^+$

13: $L_p = L_c +$?

14: return

C. Methodology

Outline: When the current location of the communication node is known, the future location of the communication node is predicted using the user mobile history.

Scheduled Time: Time slot is denoted by Δ. Scheduled time defines as the prediction about the movement of nodes. The scheduled time [17] is assigned as [Δ_{min}, Δ_{max}].

Current Time: The time of current location is denoted by [17] Δ_{curr}.

Elapsed Time: Elapsed duration in the current activity in the time slot is denoted by [19] $\Delta_{elapsed}$

Mean Time: Mean activity duration is denoted by [19] Δ_{mean}

Predicted Time: The time until which the mobility of the node is to be determined is denoted by [17] $\Delta_{predicted}$

Start the communication at initial node at time Δ

The initial node finds the next node location that is in minimum path.

If $\Delta_{min} \leq \Delta_{max,}$ take minimum path

Schedule the location using node mobile history. All the scheduling is stored in the location prediction module. Get the next activity from the node mobile history. If node moves,

Next location = current location

else

$\Delta_{curr} = \Delta_{curr} + \Delta_{mean} - \Delta_{elapsed}$

$\Delta_{curr} < \Delta_{predicted}$

Time generator is used to determine the time allotted for node. For every action inform about node movement to the node mobility module.

End

For example Figure 6 shows the mobility scenario for the wireless sensor network**.** A network containing four nodes which are S A, B and D. S is stable, A moves slowly towards S and B moves rapidly away from s and D. S needs to send a data packets to D. It finds the path to reach D.

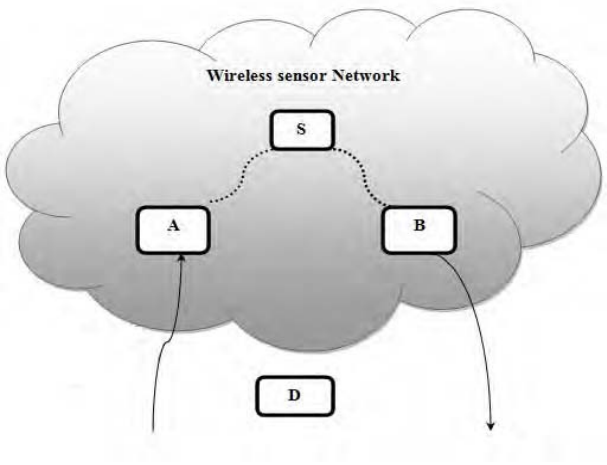

Fig.6. Mobility scenario in wireless sensor network

It has two choices, either through A or through B. If S chooses B as intermediate node, then the communication will not last long time since the link (S,B) will be rapidly broken, due to the mobility of B. But if A, takes into account the mobility of A and B, it will choose A as intermediate node because the expiration time of the link(S,A) is superior to that of (S, B). The reason for S chooses A as next hop to reach D is that the A has the greatest expiration time or the most stable path According to this example, it is clear that selecting the most stable path can avoid eavesdropping and improves routing.

VI. SIMULATION RESULTS

The simulation is carried out using Ns2 simulator. Topology is formed, in which various nodes are created. In the simulation 100 sensor nodes are randomly distributed within the network field of size 1000m * 1000m. Each node can communicate with other nodes in a radius of 50m. We indicate on average each sensor node has 40 neighbors nodes. All the movements of sensor nodes are monitored regularly by the base station. The topology used here is topography. Here AODV (Ad hoc On-Demand Distance Vector) protocol used to provide efficient communication between source and destination. The simulation results show the comparison results with existing method.

Figure 7 shows the comparison results of latency vs. simulation time. X axis indicates the simulation time, Y axis indicates the latency value. In this graph for the existing method the simulation results start at simulation time 3. At this time the latency value is 0.6. This latency value is stable till the end of the time. This is because the eavesdropper hacks the information. So there is no communication is taking place. In the proposed method shows that latency value decreases when the simulation time increases. This shows our proposed method minimize the latency.

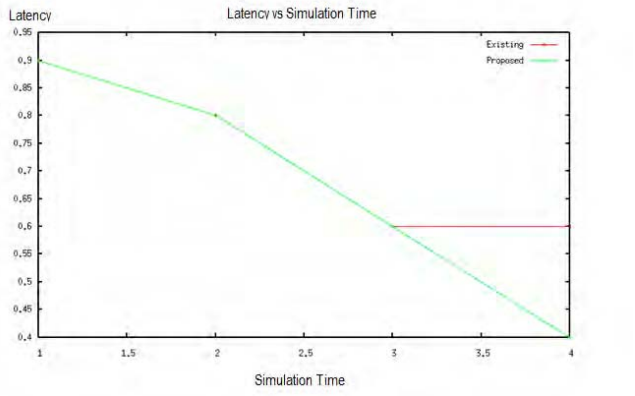

Fig.7. Latency vs. Simulation time

Figure 8 shows comparison results for the Detection ratio vs. Simulation time. The eavesdropper is identified by the energy level and characteristics of the node. For the existing method the detection ratio is high. In our proposed system the graph shows that the eavesdropper detection ratio is low. Every sensor nodes check

its neighbour node energy level. Based on the energy level the sensor node accepts the requests from the neighbor node otherwise it assumes that it is eavesdropper node, so it rejects the communication.

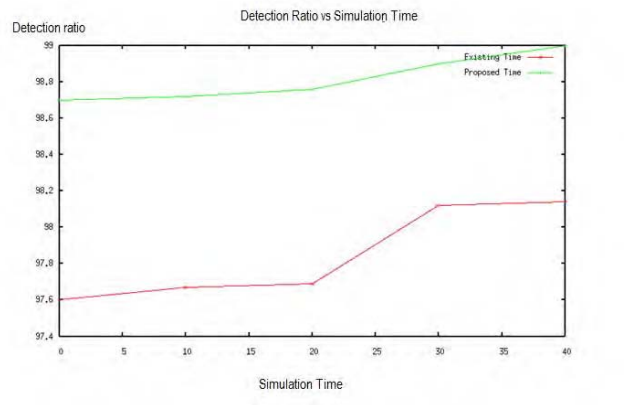

Fig. 8. Detection ratio vs. Simulation time

VII. CONCLUSION

This paper concludes that mobility prediction algorithm achieves secure data sharing between communication systems. The proposed protocols assure that it provides efficient communication between source and sink. The implemented method shows that the global eavesdropper cant able to compromise the networks. So the confidentiality of location has improved. The proposed method ensures that it can protect the location for global eavesdropper. This prediction algorithm should improve routing, and improves stability path between communication systems. This paper is evaluated the location prediction performance through analysis and simulation.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey Computer Networks", vol. 38, no. 4, pp. 393-422, 2002.
[2] Kiran Mehta, Donggang Liu, "Protecting Location Privacy in sensor Networks against a Global eavesdropper" IEEE Transaction on Mobile Computing, Vol 11,No 2
[3] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.
[4] J. Deng, R. Han, and S. Mishra, "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks," *Pervasive and Mobile Computing* J., Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.
[5] Nealpatwari" Location Estimation in Sensor Networks "
[6] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting Receiver- Location Privacy in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1955-1963, May 2007.
[7] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. Int'l Conf. Distributed Computing Systems (ICDCS '05), June 2005.
[8] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a Global Eavesdropper," Proc. IEEE Int'l Conf. Network Protocols (ICNP '07), 2007.
[9] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06), June 2006.
[10] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004
[11] T.S. Saponas, J. Lester, C. Hartung, S. Agarwal, and T. Kohno, "Devices that Tell on You: Privacy Trends in Consumer Ubiquitous Computing," Proc. USENIX Security Symp ., 2007.
[12] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM, 2008.
[13] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting Your Daily In-Home Activity Information from a Wireless Snooping Attack," Proc. Int'l Conf. Ubiquitous Computing (UbiComp '08), 2008.
[14] Hemanta Kumar Kalita, Avijit Kar" wireless sensor network security analysis"international journal of next-generation networks (ijngn),vol.1, no.1, december 2009
[15] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), 2008.
[16] Heni Kaaniche And Farouk Kamoun "Mobility Prediction in Wireless Ad Hoc Networks using Neural Networks "
[17] R.V. Mathivaruni and V.Vaidehi" An Activity Based Mobility Prediction Strategy Using Markov Modeling for Wireless Networks"