A Deviated Location and Updated Node Identity based Security Scheme for Preserving Source Node Location Privacy in Wireless Sensor Network

Neha Sahu
M.Tech Scholar
Oriental Institute of Science and Technology
Bhopal (M.P.)

Sanjay Sharma
Assistant Professor
Oriental Institute of Science and Technology
Bhopal (M.P.)

ABSTRACT

With a increased area of the applications of WSN, the security mechanisms are rising issue of outmost concern. The most important challenges threatening the successful installation of sensor systems is its privacy. Many privacy-related issues has been addressed by security mechanisms, but one sensor network privacy issue that cannot be adequately addressed by network security is source-location privacy One important class of sensor-driven applications is to monitor a valuable resources. For instance, sensors will be deployed in places like natural habitats to monitor the activities of endangered animals, or may be used in military purposes. In these asset monitoring applications, it is important to provide security to the source sensor's location. In this paper, we had proposed security scheme for preserving source node location privacy. We had developed a model assuming that attacker can monitor traffic in small area instead of whole network. Finally, we proposed a deviated location and updated node identity based scheme for efficiently protecting source node from hotspot locating attack. The protection scheme has shown the better performance which is proved by simulation results. The protection scheme has recovered the network performance in presence of attacker and provides attack free environment.

General Terms

Privacy, WSN, TCP

Keywords

Hotspot Locating Attack, DREAM, Hunter, Node identity

1. INTRODUCTION

A Wireless Sensor Network (WSN) contains hundreds or thousands of the sensor nodes. These sensor nodes are able to communicate either among each other or route the data packets hop-by-hop towards management nodes, called as sink node or base station. It is scattered over large geographical area consisting of set of sensor nodes having greater potential. Wireless Sensor Networks (WSN) [1] can be precisely defined as a cluster of sensor nodes organized in a network that are able to sense and control the environment and are deployed in regions requiring surveillance and monitoring. The sensors are deployed at a cost much lower than the traditional wired sensor system. The large number of sensors deployed will enable more accurate measurements. Even though sensor networks has various applications and advantages, but they have limitations too. They possess many threats like the energy which is a rare and non-renewable resource and the lifetime of sensor nodes i.e. they are alive only until their energy drains out completely. Moreover, it is not feasible to substitute the batteries of plenty of nodes in the network, therefore it becomes very important to boost the lifetime of sensor nodes. A Wireless Sensor Network (WSN) is a particular type of ad-hoc network. The participating nodes are smart sensors Each of these sensor nodes acquire data from surroundings, process it and route it to the sink node by multi-hopping as shown in Figure 1 [2]. The nodes exchange data in order to build a global view of the monitored region. This data is typically made accessible to the user through one or more gateway nodes [3].

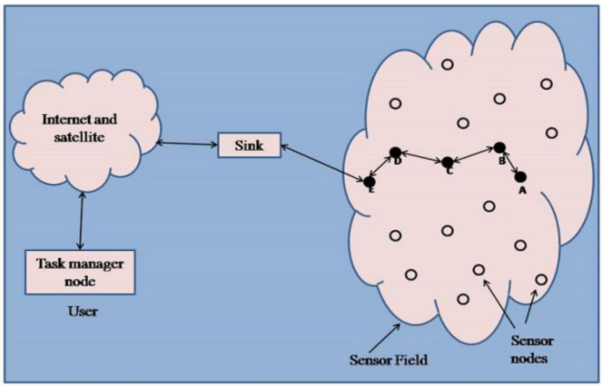

Figure 1: Basic Structure of a Wireless Sensor Network

A Sensor Node consists of one or more sensing elements (motion, temperature, pressure, etc.), a battery, low power radio trans-receiver, microprocessor and limited memory, position finding system. The block diagram of sensor node is shown in Figure 2 [2].

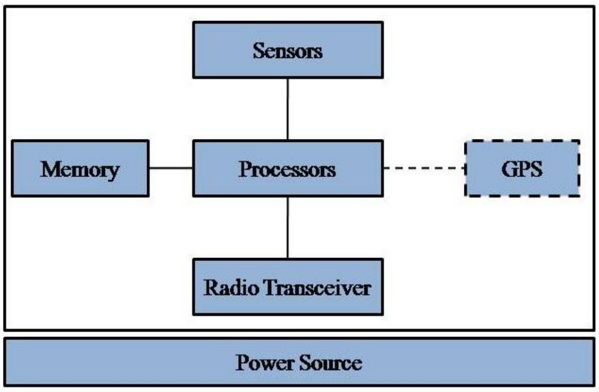

Figure 2: A basic wireless sensor network device block

A wireless sensor network (WSN) has been proposed for many applications which are useful in collection of automatic data like habitat monitoring, military surveillance etc. In this research work, I will take into account a habitat monitoring applications where the WSN is used for monitoring endangered animals. For instance, the WSN have been used by the Save-The-Panda Organization for monitoring of pandas in a wildlife sanctuary. Whenever they move in the network, their presence and activities are noticed by the sensor nodes in the network regularly and then forward the sensed data to the Sink. Since, WSNs are usually located in wide and open areas which remain unattended and also the physical boundary is absent, which makes the networks prone to various risks. In WSN, the sensed information is transmitted through open channels which makes hunter spy on the wireless link and it might use the traffic information to find source node and hunt endangered species. Thus, protecting location privacy of source nodes' is important due to the illegal use of resources available with pandas.

1.1 Constraints in WSNs

- Constraints in resource: Sensor nodes have inadequate assets such as less computational competence, insignificant memory size, poor bandwidth for wireless communication, and a exhaustible power resource i.e. non rechargeable battery.
- Reduced size of message: Sensor networks basically have message of smaller size in comparison to the other existing networks. Therefore, there is no need of doing segmentation in various applications of WSN.
- Addressing Schemes: Since, WSN consists of thousands number of sensor nodes comparatively to other network, thus, it is not at all possible to build global addressing technique for working of a huge number of sensor node because the overhead incurred in maintaining identity is more.
- Redundant Data and Location of sensors: Alertness regarding the position of sensor node plays a very crucial role because data collection is mostly dependent on it. Moreover, there might be some other common phenomena of collecting data, so there is a huge probability that some duplicity must be present in this data.

1.2 Security Requirements

The objective of security services provided in WSN is to safeguard the data (i.e. facts and figures) and assets from adversary and some unusual behavior. The security requirements included in WSN are as mentioned below:

- Data Authentication: It must be checked that the data is initiated from the exact source.
- Data Confidentiality: It must be made sure that only allowed sensor nodes can get access to the content of the messages.
- Data Integrity: It must be made sure that no modification has been done to the received message by any unauthorized parties.
- Availability: It must be made sure that the services which are being offered by WSN or any node must be available whenever required.
- Data Freshness: It must be made sure that old data have not been replayed.
- Authorization: It must be made sure that only legitimate sensor nodes must be able to give information to network services.
- Non-repudiation: It must be made sure that a node cannot deny for sent message which it has sent previously.
- Robustness: It must be made sure that even when few nodes are damaged, the entire network should function properly.
- Privacy: It must be made sure that information sensed stays within the WSN and is only accessible by the trusted parties.

1.3 Privacy in WSNs

Privacy is one of the most important challenges intimidating on the horizon which threatens the successful operation of sensor networks. Privacy can be defined as the assurance that information, in its universal sense, is visible or understandable by only those whom are purposely meant to examine or decipher it. The phrase "in its universal sense" is meant to entail that there might be types of information besides the message content that are associated with a message transmission. Therefore, the threat that prevails against the privacy of sensor networks are classified as: content-oriented threats, and contextual threats. Content-oriented security and privacy threats are issues which arises due to the ability of the antagonist to monitor and control the precise content of packets being sent from one network to other and the packets might consists of actual sensed-data or simply some other lower-layer control information. Moreover, issues of Contextual privacy related with transmission of messages in sensor network, have not been addressed yet. Whereas the contextual privacy is agitated with safeguarding the context related with the evaluation and broadcasting of sensed data. For various applications of WSN, contextual information of surrounding environment like the location of the original message source, are very sensitive and hence must be protected. This is very important when the sensor network is used for monitoring valuable assets because securing the location of resources becomes crucial. There are two types of privacy in WSN, commonly called as:

- Source location privacy (SLP): It focus on the protection of the source node's location which reports physical activities happening in their surroundings. Note that the antagonist is not usually concerned in finding the device to interfere with it but to be able to find out the location of the events occurring nearby.
- Receiver location privacy (RLP): It concentrates on safeguarding of the destination's location which is a repository of all data packets of the network The attacker is only interested in searching the location of sink node as it is the most valuable assets of the sensor network and if it's security is compromised, the complete network will be under the control of the adversary.

2. RELATED WORK

Security schemes are providing a free environment from malicious nodes or attacker nodes in network. This section presents the some latest techniques.

In this paper [5] firstly they had defined a hotspot phenomenon which shows an inconsistent flow in traffic pattern of the network because of the huge amount of packets coming from a trivial area. Secondly, they had develop a realistic local adversary model, in which adversary can continuously monitor and analysis the traffic pattern of network in small multiple areas, instead of the complete network . They had introduced an attack known as Hotspot-Locating attack in which the attacker uses traffic analysis techniques to locate hotspots. Finally, they had proposed a cloud-based scheme for efficiently protecting source nodes' location privacy against Hotspot-Locating attack by creating a cloud with an irregular shape of fake traffic, to counteract the inconsistency in the traffic pattern and camouflage the source node in the nodes forming the cloud.

In this paper[6**]** PRIPO stands for **P**rivacy-**P**reserving **R**outing and **I**ncentive **P**r**O**tocol for hybrid ad hoc wireless network. It can facilate node cooperation in the network and protects the users' locations privacy and communication activities through lightweight hashing and symmetric-key-cryptography techniques without submitting receipts. The nodes' alias name are accurately calculated using hashing methods. Only trusted parties can link these pseudonyms with the actual identities for charging and rewarding operations.

According to [7], they proposed a location privacy routing protocol (LPR) that is easy to implement and provides path diversity. When the actual network traffic is combined with injection of fake packet, routing protocol minimizes the traffic direction information that an attacker can retrieve via eavesdropping. The uniform distribution of directions of both incoming and outgoing data traffic at a sensor node by the new defense system makes it very difficult for an opponent to do analysis on information gathered locally and interpret the direction of the sender and receiver.

In this title[8], they proposed a scheme to preserve the location privacy of Sink's node from the traffic-rate analysis attacks. The anti-traffic analysis techniques introduced in this system randomizes traffic volumes of data packets throughout the network away from the base station, so that the adversary can be deceived and misdirected and the way towards the base station cannot be easily searched.

In this title[9], they had proposed the phantom Flooding/ Routing scheme in which they had achieved location privacy by making every packet generated by a source walk a random path which is either pure random walk or directed walk which let the messages towards the phantom source. Then the single path routing or flooding is employed to route the message toward the destination. As every message follows different path, this results in the increased safety period against local eavesdropper.

In this title [10], they aims to maintain source privacy under eavesdropping and node compromise attacks (SPENA).They proposed a routing protocol to hide information of source node using cryptographic techniques having less overhead. The modification is performed during routing by selecting nodes randomly in a path to make it tough for an adversary to trace the packet back to a source node and also prevent packet spoofing. This is necessary because the adversary model takes into account a super-local eavesdropper which has the capability to compromise the nodes.

In this title [11], they proposed new Timed Efficient Source Privacy Preservation (TESP2) scheme against a global adversary who can monitor and analyze all traffic over the entire network. It introduced a new privacy scheme in which each sensor node will broadcast data collection request to its upstream nodes at a regular interval of time, and every upstream node will send the cipher text of real data if it has sensed an event otherwise it will send the cipher text of fake packets. After getting the cipher texts of real data from upstream nodes, the sensor node encrypts them twice and sends them to their downstream node. With this privacy scheme, the source of original data gets hidden, and the privacy of source node is achieved.

3. PROPOSED PROTECTION SCHEME

The aim of proposed scheme is to provide the source location privacy against hotspot locating attack in Wireless Sensor Network. In this thesis, we had provided privacy against the attack by misguiding attacker by sending him the deviated location information and false identity of the sensor nodes. In the proposed work, the adversary deploys the monitoring nodes in the WSN, we will called them as attacker in our entire work. The attacker continuously monitors the traffic of particular area of the entire network. The attacker collects the traffic information which includes the unique identity of the node, its location (x-y co-ordinates), time at which the information is last updated and the speed of the mobile node. It collects this information of mobile nodes through DREAM protocol. On the basis of this information, it attacks the nodes by sending the false reply of route existence from sender to receiver and drops all the data packets.

In order to protect the source node from the attacker, the protection scheme has been applied. In protection scheme, all the nodes are aware about the behaviour of attacker in the network. Now, whenever attacker uses DREAM protocol to know the information of the nodes in its range, all the nodes send their deviated location and false identity of the node to misguide the attacker. Therefore, the entries in the location table of attacker contain false information of the location and identity of the node. Now, whenever the attacker tries to attack the source node on the basis of entries in its location table, it does not succeed in doing so because it attacks on the deviated location of the node and hence the source node gets protected from the attack. It attacks somewhere else in the network other than the destined node. In this way, the data packets have been sent successfully from the source to the sink.

3.1 Proposed Algorithm

The proposed algorithm of security scheme is given the whole steps misguide the attacker in and provides secure data delivery in network.

```
Initialize
    S: Sender Nodes
    $S_s$: Sink Node
    Attack Type : Hot Spot Location Attack
    Attacker Uses: Dream Protocol (for location and
Capturing)
    Normal Routing: AODV
    Prevention: Location and Id Updating
    Step 1: Begin
Step 2: Source Node detects the event
Step 3: Source Node S Search Sink $S_s$ Node for Message
Transfer
Step 4: If ($S_s$ found and Attacker present network)
            {
```

```
        Capture Location and id of S node using Dream
        Target to Source S
        }
        Else If ($S_s$ found and Source S send updated Location and ID info and Attacker present network)
    {
          Capture Location and id of S node using Dream
          Target to Source S
          Target not found
           Safe Data send to Sink $S_s$
    }
      Else
      {
        Normal Data Delivery to $S_s$ sink Node
      }
Step 5: Stop
```

3.2 Proposed Flow Chart

The flow chart of the algorithm of the proposed work is as shown in the Figure 3.

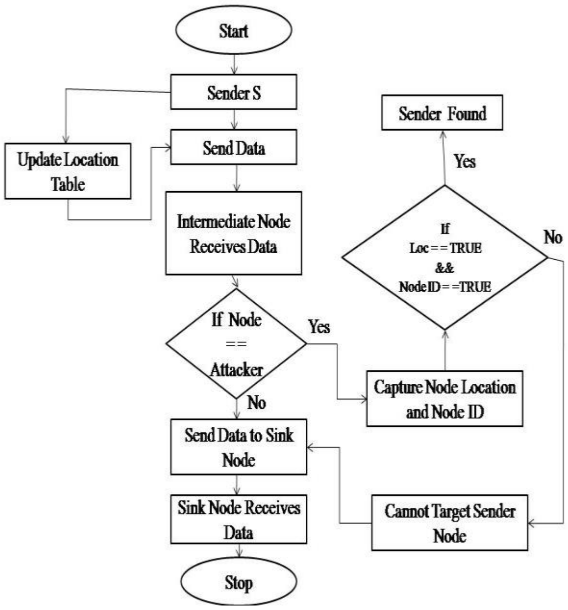

Figure 3: Flow Chart of Proposed Algorithm

4. SIMULATOR DESCRIPTION

The simulation is implemented In Network Simulator 2.31 [12], a simulator for mobile ad hoc networks. The simulation parameters are provided in Table 1. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, the simulation time is 100, and then moves to another random position with a velocity chosen random and maximum up to 30 m/s. A packet size of 512 bytes and a transmission rate of 3 packets/s.

Table 1. Simulation Parameters for Case Study

Routing Protocol	AODV
Number of nodes	50
Dimension of simulated area (metre)	800×800
Simulation time (seconds)	100
Sensor nodes transmission range (metre)	550
Traffic type	CBR, 3pkts/s
Packet size (bytes)	512 bytes
Number of traffic connections	TCP/UDP
Maximum Speed (m/s)	30
Node movement	Random
Types of attack	Hotspot Location attack

5. SIMULATION RESULTS

In this section the analysis of simulation results are mentioned with the scenario of normal routing, in case of attack and when protection scheme is applied.

5.1 Routing Load Analysis

The routing packets are required in network to find the destination and confirm the path in between source and destination. The destination is validating the request packets then after that the data packets in network is delivered. This graph represents the routing packets analysis in case of attack and protection scheme. This graph illustrate that in case of attack about 1700 packets are deliver in network but on the other hand in case of protection scheme about 6500 routing packets are deliver in network. The less amount of routing packets delivery provides the better performance in network. In case of attacker or hunter very few packets are send in network but in case of protection the packets quantity is more. The attacker aim is to identify the node ID in network and after that attacker convey false reply of route existence to destination. The attacker is identifying the location of source nodes and drops the data packets in network. The proposed deviated location and node identification (ID) scheme is provides the attacker free environment and secure path for data delivery.

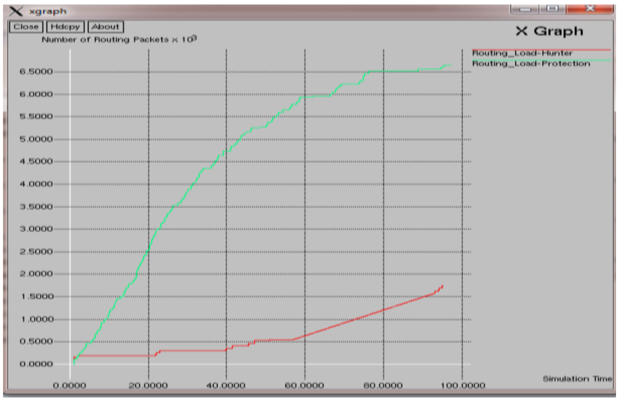

Figure 4: Routing load Analysis

5.2 PDR Analysis

Packet Delivery Ratio (PDR) is the performance metrics that measures the percentage of data successfully received at destination. In healthy network the performance of PDF is always fine and also possible to reaches at 100% for certain time duration. The presence of attacker in network i.e. also called Hunter consider in this research identified the location of mobile nodes and then drop the packets in network of particular node id. The attacker has degrades the network performance that is clearly shown in this graph, only 4% of data is received at destination up to the end of simulation. In case of protection the network performance has overcome and provides the 90 % PDF at the end of simulation and it is at least about 85% in network. It means the protection scheme has improved the performance of network in presence of attacker.

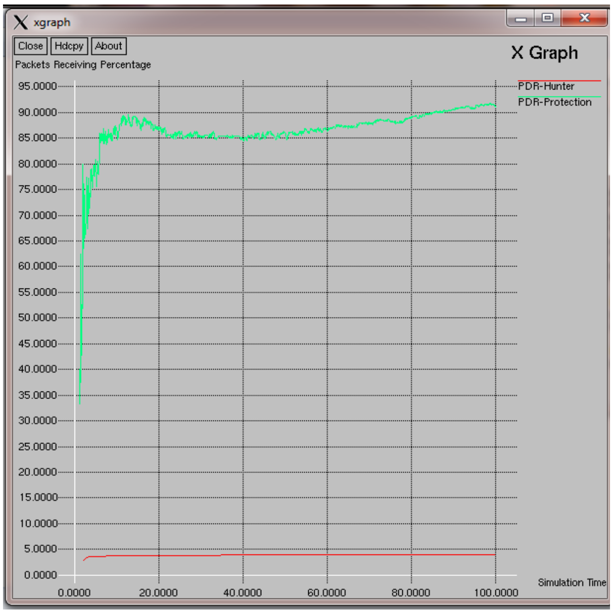

Figure 5: PDR Analysis

5.3 Attacker Loss Analysis

In network, the aim of attacker is to damage the network and degrades it's performance time to time in network. In this research, the attacker has targeted the nodes on the basis of their location and node-ID in network. The attacker has identified the location of node through the location table and then targets the source node. The attacker has identified the actual position and state of node and then drops all data packets that had originated from the source node. In this graph, the analysis of packet delivered to the sink node has been mentioned in the presence of attacker. It is described as how much amount of data packets has been lost in a given simulation time. This graph has illustrated the data loss in network in presence of hunter and evaluated the loss of data.

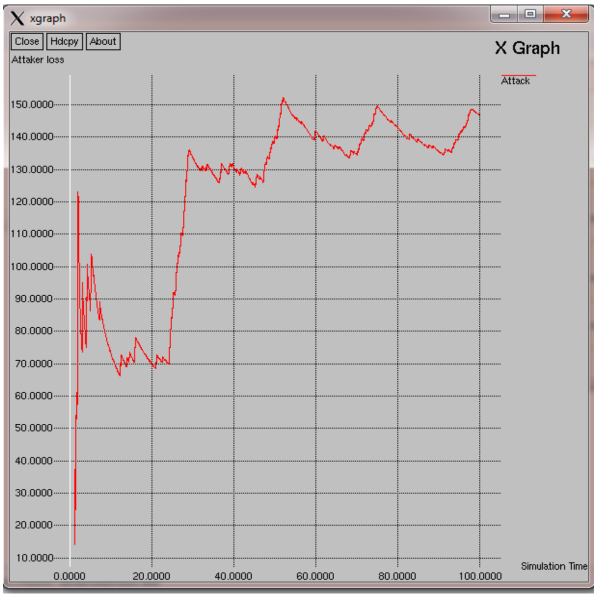

Figure 6: Attacker Loss Analysis

5.4 UDP Packet Receive Analysis

The UDP (User datagram Protocol) is the second category of transport protocol which has followed the connection less mechanism for end to end communication in network. This protocol has directly delivered the packets without any confirmation of successful delivery in network, because of that this protocol is also unreliable for communication. This graph is appraised the packet receiving analysis during the attack and during the protection scheme in WSN. Here in presence of attack about 120 packets are received in network but in case of protection scheme about 280 packets are received in network. The protection scheme is really effective and recovers the network performance in presence of attack. The false ID information for attacker works in favor of protection scheme by that the attacker is unable to identify the actual ID of node in the network.

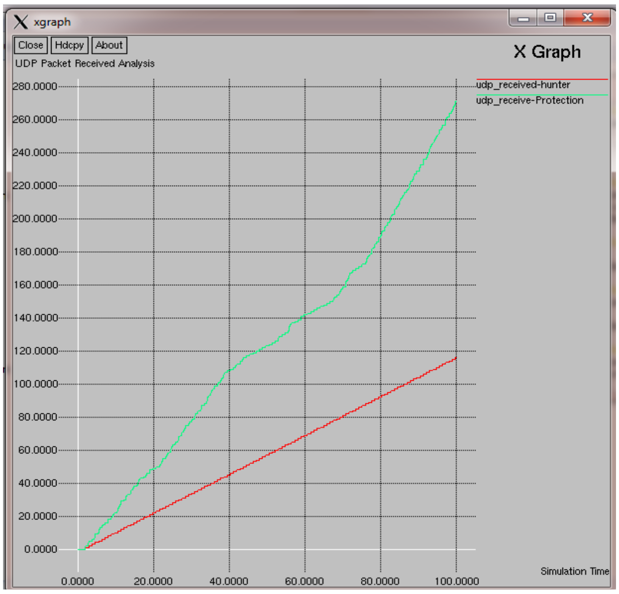

Figure 7: UDP Packet Receive Analysis

5.5 TCP Analysis in case of Hunter

TCP (Transmission Control Protocol) is the most reliable protocol for communication in network because of their connection oriented mechanism. If the sender in network is sending the packets using TCP, then the next transmission of sender depends on the successful delivery confirmation through ACK (Acknowledgement) packets of first transmission. The TCP packets are also called the "congestion window". Theses window size is random but also depends on the delivery of packets in network. This graph appraised the performance of TCP congestion window in case of attack. Here we apparently scrutinized the performance of four TCP connections insignificant in network. It means the attacker fully humiliates the network performance of TCP protocol in attacker affected network.

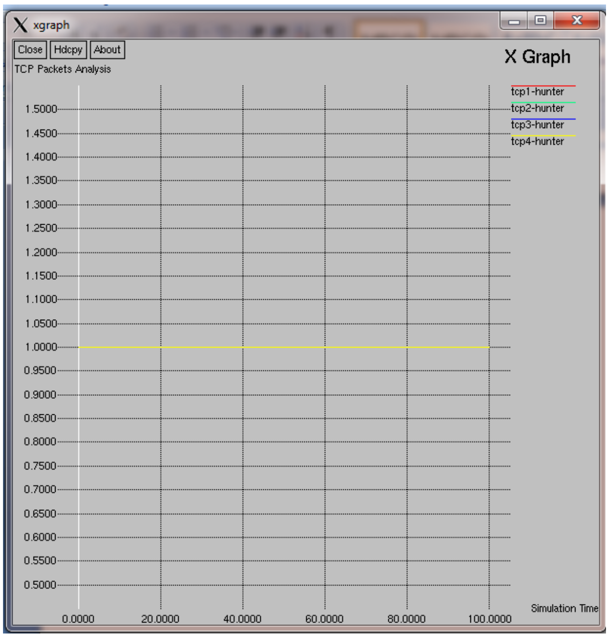

Figure 8: TCP Hunter Analysis

5.6 TCP Analysis in case of Protection Scheme

The reliability of TCP protocol is scrutinized through this graph. In this graph the performance of TCP congestion window of all connections is assessable and apparently noticeable in network. The TCP 4 connection is represents the highest size of congestion window, it is about 36 packets at time of 70 seconds in network. The performance of rest of the connections is also satisfactory. The protection scheme is immobilize the attacker capability of finding the nodes on the basis of their location table. It means if the nodes ID wrong forwarded to attacker then in that case it confused about that new ID on its own location table and should be not possible to attack on node/s in network. The protection scheme is improves the network performance and also disable the affect of attacker in network.

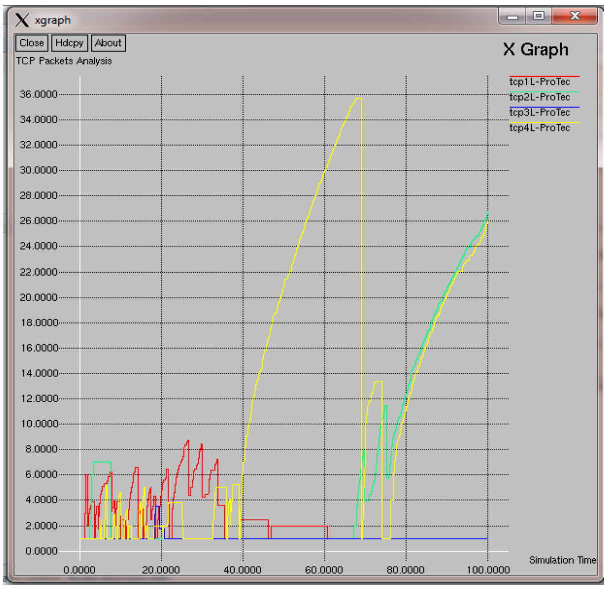

Figure 9: TCP Protection Analysis.

5.7Analysis of Updated Node Identity

During the data communication in WSN, to protect the privacy of source node from adversary, it always transmits its updated node identity to the other nodes present in the network. Since there are 50 nodes in our simulation, therefore source node update its value by 49. Table 5.4 shows the actual sender id, updated sender id and the receiver id. The sink node is the receiver of all data packets. Sink node is assigned a value 0. The node 1, 9, 12, 17, 34 and 40 are source nodes in our simulation environment and their updated node identities are as follows:

Table 2. Table containing actual and updated sender nodes identity

Actual Sender Id	Updated Sender Id		Receiver Id	Total Packets Received
1	50	→	0	504
9	58	→	0	0
12	61	→	0	21
17	66	→	0	356
34	83	→	0	1222
40	89	→	0	283

5.8 Analysis of Location Table of Hunter

The attacker in the network maintains a location table using DREAM Protocol. The table consists of node address (node-id), location(x-y co-ordinates), speed and the time information was last updated. Using this information stored in the table, the attacker attacks the source node. The table and Table 5.4 shows the Location tables of two different monitoring nodes at the same time. The table contains the information of its neighbouring nodes, when proposed protection scheme is not applied. The sensor node sends actual information of their location and node id. With the help of this information, monitoring nodes can interact with each other and attacks the target node. The highlighted row shows that location of node 12, 24, 48 are same in the location table of two monitoring nodes. The node 12 is a source node in the simulation environment.

Table 3. Location Table of hunter node 35 before protection scheme

Address	Time	X	Y	Speed
4	2.03107	600	350	0
7	4.96348	80	200	0
12	1.55679	580	510	0
18	3.2061	600	550	0
24	4.03056	768.71	11.0237	11
26	7.11006	679.397	163.821	15
27	2.88029	787	200	0
28	3.89204	800	300	0
29	5.17791	720	380	0
30	9.68554	616.551	409.516	15
31	4.41763	800	500	0
32	1.84994	700	550	0
33	9.38189	699.766	567.57	8
40	5.6597	800	600	0
48	5.12916	133.489	548.949	15

Table 4. Location Table of hunter node 19 before protection scheme

Address	Time	X	Y	Speed
1	3.22844	450	550	0
5	5.02494	380	520	0
6	5.83408	400	510	0
7	4.96348	80	200	0
9	4.57469	200	520	0
12	1.55679	580	510	0
17	4.77546	450	500	0
18	3.2061	600	550	0
24	4.03056	768.71	11.0237	11
26	7.11006	679.397	163.821	15
27	2.88029	787	200	0
30	9.01888	626.392	411.293	15
32	1.84994	700	550	0
38	2.76107	400	590	0
43	2.62494	400	500	0

After the protection scheme has been applied, the sensor nodes send their different location id and updated node address to the monitoring nodes at time. This misguides the attacker from attacking the target node since they get different values at the same time. Table 5 and Table 6 shows the location table of monitoring nodes after protection scheme has been applied The entries of location of nodes 7, 24 are different for both monitoring node at the same time. The node 12 which is a source node sends its updated identity to the hunter node. The hunter when tries to attack on the source node using values from its location table, it attacks somewhere else in the network and hence, the source node gets preserved. The highlighted row shows the information of source node 12 during protection scheme.

Table 5. Location Table of hunter node 35 after protection scheme

Address	Time	X	Y	Speed
4	2.03107	138.027	76.9098	0
7	4.96348	4.5806	59.899	0
61	1.55679	8220	126.642	0
18	3.2061	779.763	552.94	0
24	4.03056	571.721	5.04564	42.7352
26	7.11006	710.858	382.967	0.56977
27	2.88029	1562.95	21.8162	0
28	3.89204	53.0074	29.394	0
29	5.17791	812.605	747.642	0
30	9.68554	629.302	488.843	67.3696
31	4.41763	1580.45	119.668	0
32	1.84994	1591.55	539.039	0
33	9.38189	2072.75	2926.41	19.6022
89	5.6597	22340.8	432.264	0
48	5.12916	85.744	1395.62	7.0911

Table 6. Location Table of hunter node 19 after protection scheme

Address	Time	X	Y	Speed
50	3.2284	150.036	819.95	0
5	5.02494	178.115	75.7036	0
6	5.83408	779.399	34.0006	0
7	4.96348	11.1537	377.287	0
58	4.57469	120.855	880.257	0
61	1.55679	865.818	2304.99	0
66	4.77546	1115.4	1322.36	0
18	3.2061	4810.68	880.274	0
24	4.03056	649.677	1.63391	28.9048
26	7.11006	709.802	387.233	12.5454
27	2.88029	914.214	41.9562	0
30	9.01888	528.068	409.726	17.1605
32	1.84994	380.235	22.432	0
38	2.76107	476.344	41.3429	0
43	2.62494	537.27	564.072	0
48	5.12916	64.1501	819.575	19.2536

5.9 Performance Metrics:

In our simulations, we have used several performance metrics to compare the performance of our system during the hotspot locating attack and after the prevention measures has been applied. The following metrics were considered for the comparison.

5.9.1 Packet delivery fraction (PDF): The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.

5.9.2 Normalized routing load: Measured as the number of routing packets transmitted for each data packet delivered at the destination.

5.9.3 UDP received analysis: The UDP received analysis is depends on the number of UDP packets are received in destination in case of attack and after applying security scheme.

5.9.4 TCP packets analysis: TCP packets of TCP congestion window are measure in case of attack and proposed security scheme.

Table 7 shows the overall summery of the performance metric. It shows the comparison of various parameters when the attack has been launched without any protection scheme and when the protection scheme has been applied to the network. This table shows the effectiveness of our proposed protection scheme.

Table 7. Summary of Results

Parameter	Before	After
Send Packets	2969	2386
Receive Packets	116	2164
Routing Packets	1752	6661
PDF	3.91	90.70
NRL	15.10	3.08
No. of dropped data packets	2853	222

6. CONCLUSION

Security is another unique characteristic of WSN and it is a fundamental concern in order to provide protected and authenticated communication between sensor nodes in critical applications, such as military or healthcare. In WSN, physical security of sensor nodes is not granted as they are usually deployed in remote and hostile environments. Therefore, attackers can easily compromise sensor nodes and use them to degrade the network's performance. In order to optimize the conventional security algorithms for WSN, it is necessary to be aware about the constraints of sensor nodes. In this research, the Attacker identifies the hotspot location and it has the location and id information of all nodes within its range through location based DREAM protocol and it attacks the also blocks their communication activity in network. Our protection scheme provides the attack free environment in presence of attacker and it also improves the network performance.

7. FUTURE WORK

In our simulation environment, we had secured the privacy of location of source node from the Hot Spot Location attack using deviated location and updated node identity method, but in future we also enhanced that work with the help of collaborative decision making system approach so as to make our work more precise. In future we also try to implement security at application layer level.

8. ACKNOWLEDGMENTS

I am grateful for the valuable guidance and support of my Project Guide Mr. Sanjay Sharma without whom all my effort would have been directionless and fruitless. I sincerely thank them, for assisting me in completing the work.

9. REFERENCES

[1] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks", Attacks and Countermeasures", Ad Hoc Networks (elsevier), Page: 299-302, 2003.

[2] C.Y. Chong and S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," in IEEE Proceedings, pp. 1247–1254, Aug.2003.

[3] Santi, P. "Topology control in wireless ad hoc and sensor networks" Chichester, England: John Wiley & Sons, 2005.

[4] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[5] Ipsita Panda "A Survey on Routing Protocols of MANETs by Using QoS Metrics" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012.

[6] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, " A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 10, pp. 1805-1818, October 2012.

[7] M. Mahmoud and X. Shen, "Lightweight Privacy-Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Networks," Proc. IEEE INFOCOM '11-Int'l Workshop Security in Computers, Networking, and Comm. (SCNC), pp. 1006-1011, Apr. 2011

[8] 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.

[9] J. Deng, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," Proc. Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm), pp. 113-126, Sept. 2005.

[10] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy Constrained Sensor Network Routing," Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04), pp. 88-93, 2004

[11] K. Pongaliur and L. Xiao, "Maintaining Source Privacy Under Eavesdropping and Node Compromise Attacks," Proc. IEEE INFOCOM, Apr. 2011.

[12] R. Lu, X. Lin, H. Zhu, and X. Shen, "TESP2: Timed Efficient Source Privacy Preservation Scheme for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm., May 2010.

[13] Network Simulator- ns-2. http://www.isi.edu/ nsnam /ns/

.