www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 4 April 2017, Page No. 21131-21135
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.57

Data Integration among Sensor Nodes Using Wireless Toolkit

K. David Raju [1], *Shreya Valluri*[2], *V Harika Naidu*[3]

[1] Associate professor of Computer Science dept., St. Peter's Engineering College, Hyderabad,
davidraju@stpetershyd.com
[2]Student of Computer Science dept., St. Peter's Engineering College, Hyderabad,
shreya.valluri1@gmail.com
[3]Student of Computer Science dept., St. Peter's Engineering College, Hyderabad,
harrynk1.0@gmail.com

Abstract: ***Network level privacy can be categorized into four sub categories: Identity, route, location and data pivacy.It is so challenging to achieve complete network level privacy due to the constraints like energy, memory and computation power imposed by the sensor nodes and constraints like mobility and topology imposed by the sensor networks and QOS issues like packet reachability and timeliness. In this paper we proposed a new identity routing and location algorithm that provides additional reliability and data privacy.This proposed solution protects the data from various privacy attacks such as eavesdropping and hop-by-hop trace back attacks.***

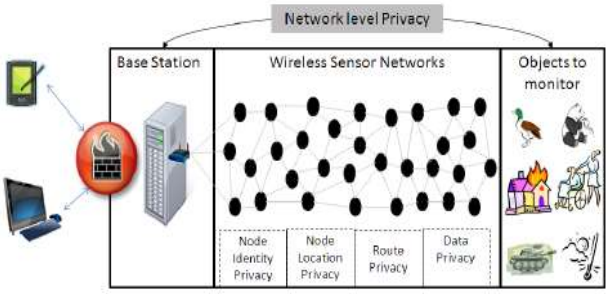
Keywords: wireless sensor networks, privacy, eavesdropping, hop-by-hop trace back.

1. Introduction

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analyzed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the on-board sensors start collecting information of interest.

Wireless sensor devices also respond to queries sent from a "control site" to perform specific instructions or provide sensing samples. The working mode of the sensor nodes may be either continuous or event driven. Global Positioning System (GPS) and local positioning algorithms can be used to obtain location and positioning information. Wireless sensor devices can be equipped with actuators to "act" upon certain conditions.

Figure 1. Typical WSN scenario.



WSNs were initially designed to facilitate military operations but its application has since been extended to health, traffic, and many other consumer and industrial areas. A WSN consists of anywhere from a few hundreds to thousands of sensor nodes. The sensor node equipment includes a radio transceiver along with an antenna, a microcontroller, an interfacing electronic circuit, and an energy source, usually a battery. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust. As such, their prices also vary from a few pennies to hundreds of dollars depending on the functionality parameters of a sensor like energy consumption, computational speed rate, bandwidth, and memory.

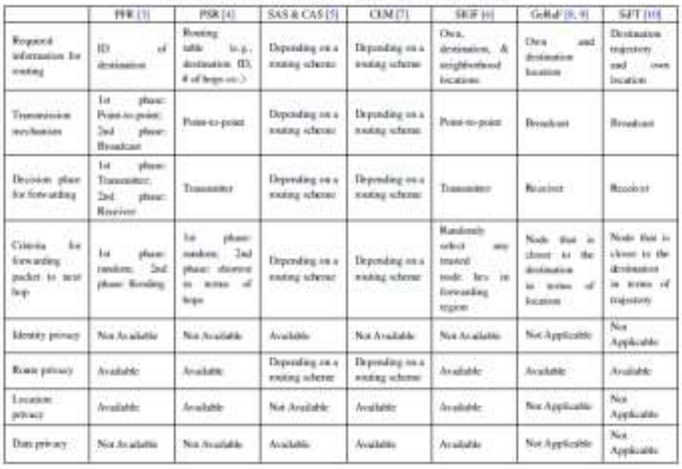
2. Literature survey

Wireless Sensor Network basically consist of numerous sensors nodes and the wireless channel to connect the nodes and each node mainly consists of trans receiver section, ultra-low power digital signal processor or microcontroller/microprocessor, external memory , various interfaces for data collection and power section. Number of nodes in any network varies from hundreds to thousands which makes it different than other wireless networks and therefore WSN is complex and challenging to control and maintain on continuous basis. As data is moving from various sensor nodes in the network the issues related to sensor data collection, data formatting, data transfer, data speed, data security and privacy, power optimization and power management, memory space and computational limitations, time delay and synchronization of the complete process and other related aspects opens new fields of research. Wireless Sensor Network works in environment conditions especially where wired connections are not possible. Wireless sensor nodes consists of different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of physical and environmental conditions.

The privacy schemes that have been proposed for wireless sensor networks are

- Phantom routing scheme which prevents the attacker from knowing the location of the source[1].The major advantage of this scheme is source location privacy protection.
- Phantom single-path routing scheme in which a packet will be forwarded to the destination using a single path routing strategy such as shortest path routing[2].
- Simple anonymity scheme which uses dynamic pseudonyms instead of true identity during communications but it is not memory efficient[3].
- Cryptographic Anonymity scheme which uses keyed hash functions to generate pseudonyms. It is memory efficient but it needs high computation power[3].
- Cyclic Entrapment method which minimizes the chance of finding out the source node location[4].
- Geographic random forwarding scheme is based on broadcast transmission. The sender only requires the position of source and the destination[5,6].
- Simple forwarding over trajectory scheme is based on broadcast transmission and doesn’t maintain neighborhood position and states[7].
- Secure implicit geographic forwarding scheme is based on implicit geographic forwarding protocol. This protocol provides data, route and location privacy[8].

Table 1. Comparison of privacy preserving schemes.



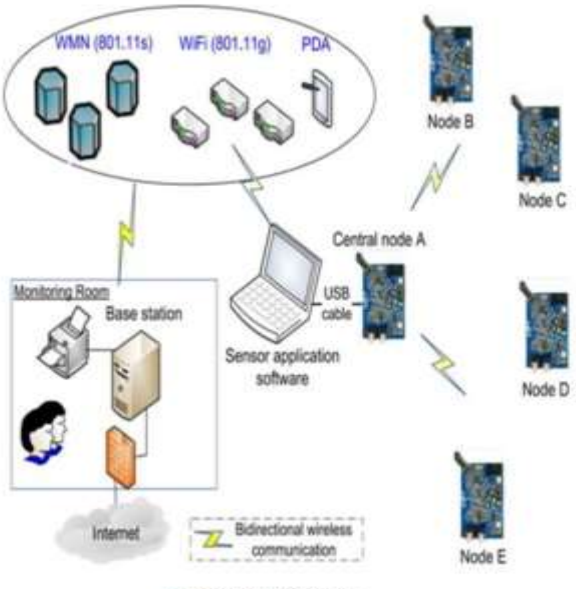
	PFR [1]	PSR [4]	SAS & CAS [5]	CEM [7]	SIGF [6]	GeRaF [8, 9]	SFT [10]
Required information for routing	ID of destination	Routing table (e.g., destination ID, # of hops etc.)	Depending on a routing scheme	Depending on a routing scheme	Own, destination, & neighborhood locations	Own and destination location	Destination trajectory and own location
Transmission mechanism	1st phase: Point-to-point; 2nd phase: Broadcast	Point-to-point	Depending on a routing scheme	Depending on a routing scheme	Point-to-point	Broadcast	Broadcast
Decision place for forwarding	1st phase: Transmitter; 2nd phase: Receiver	Transmitter	Depending on a routing scheme	Depending on a routing scheme	Transmitter	Receiver	Receiver
Criteria for forwarding packet to next hop	1st phase: random; 2nd phase: flooding	1st phase: random; 2nd phase: shortest in terms of hops	Depending on a routing scheme	Depending on a routing scheme	Randomly select any trusted node lies in forwarding region	Node that is closer to the destination in terms of location	Node that is closer to the destination in terms of trajectory
Identity privacy	Not Available	Not Available	Available	Not Available	Not Available	Not Applicable	Not Applicable
Route privacy	Available	Available	Depending on a routing scheme	Depending on a routing scheme	Available	Available	Available
Location privacy	Available	Available	Not Available	Available	Available	Not Applicable	Not Applicable
Data privacy	Not Available	Not Available	Available	Available	Available	Not Applicable	Not Applicable

3. Proposed work

A new Identity, Route and Location (IRL) privacy algorithm is proposed that ensures the anonymity of source node’s identity and location. It also assures that the packets will reach their destination by passing through only trusted intermediate nodes.

A wireless sensor network (WSN) is composed of large number of small sensor nodes that are of limited resource and densely deployed in an environment. Whenever end users require information about any event related to some object(s), they send a query to the sensor network via the base station. And the base station propagates that query to the entire network or to a specific region of the network. In response to that query, sensor nodes send back required information to the base station. Links are bidirectional. Also, sensor nodes use IEEE 802.11 standard link layer protocol, which keeps packets in its cache until the sender receives an acknowledgment (ACK). Whenever a receiver (next hop) node successfully receives the packet it will send back an ACK packet to the sender. If the sender node does not receive an ACK packet during predefined threshold time, then the sender node will retransmit that packet.

4. Implementation

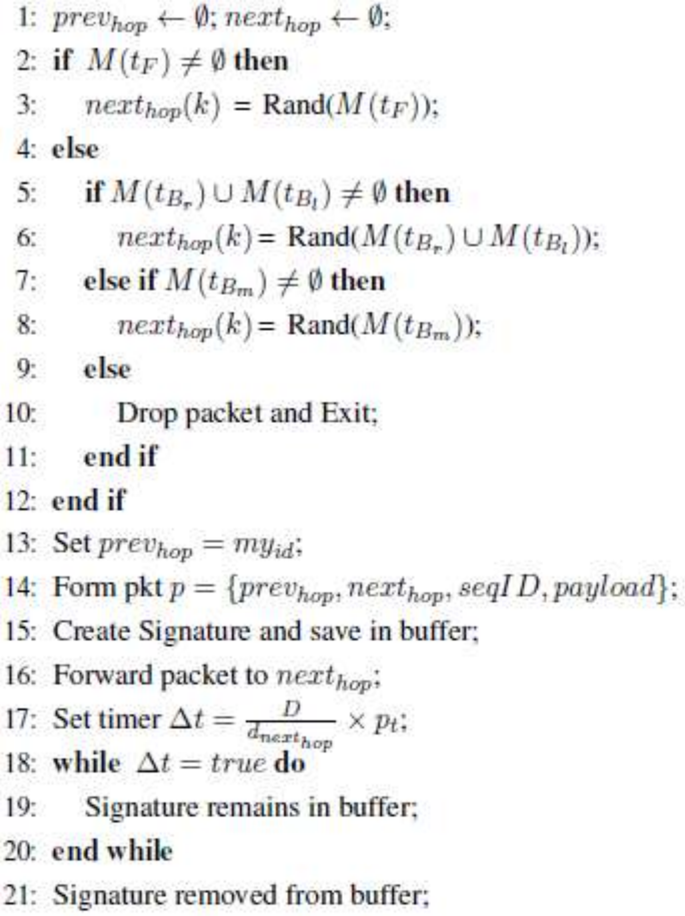


basic block diagram of WSN

A wireless sensor network is quite simply a handsome number of wireless sensor nodes set in one or the other network format (for example mesh or star).

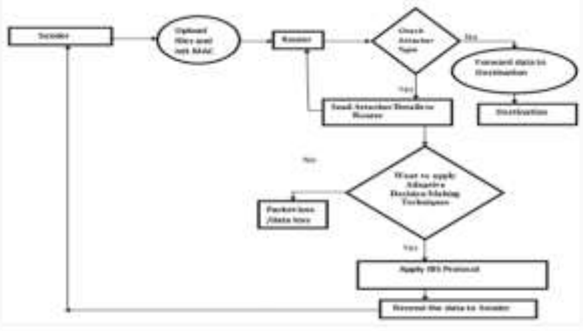
- These wireless sensors can be used to monitor either physical or environmental conditions like temperature, sound pressure, etc.
- They are capable of taking the reading and passing their data through the network to a main or center location.
- Such networks initially came into existence as a military application for battlefield surveillance and is today being used in many industrial and consumer applications.
- It is important to note the several design factors that have been laid out by many researchers.
- The ability or a sensor node to maintain the sensor network functionalities without any interruption caused due to sensor node failures can be considered as a measure of its reliability.
- There are many reasons why sensor nodes fail. For example they may fail due to the lack of energy, due to physical damage, inactivity, a communication problem and even environmental interference.

Algorithm



```
$prev_{hop} \leftarrow \emptyset; next_{hop} \leftarrow \emptyset;$
if $M(t_F) \neq \emptyset$ then
    $next_{hop}(k)$ = Rand($M(t_F)$);
else
    if $M(t_{B_r}) \cup M(t_{B_l}) \neq \emptyset$ then
        $next_{hop}(k)$ = Rand($M(t_{B_r}) \cup M(t_{B_l})$);
    else if $M(t_{B_m}) \neq \emptyset$ then
        $next_{hop}(k)$ = Rand($M(t_{B_m})$);
    else
        Drop packet and Exit;
    end if
end if
Set $prev_{hop} = my_{id}$;
Form pkt $p = \{prev_{hop}, next_{hop}, seqID, payload\}$;
Create Signature and save in buffer;
Forward packet to $next_{hop}$;
Set timer $\Delta t = \frac{D}{d_{next_{hop}}} \times p_t$;
while $\Delta t = true$ do
    Signature remains in buffer;
end while
Signature removed from buffer;
```

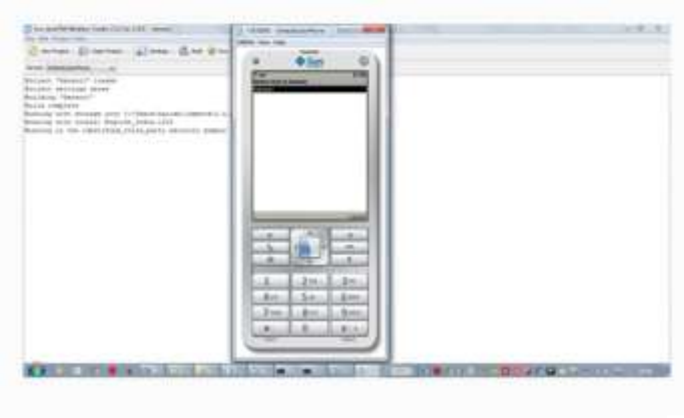
DATA FLOW Diagram



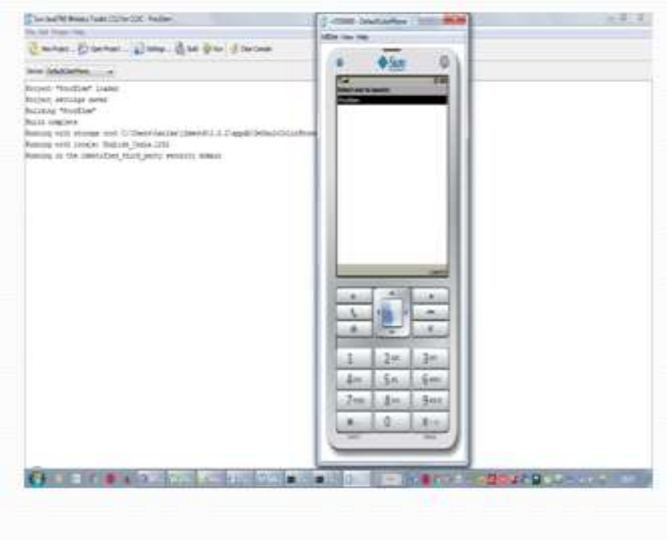
Data Flow Diagram

5. Result and Analysis

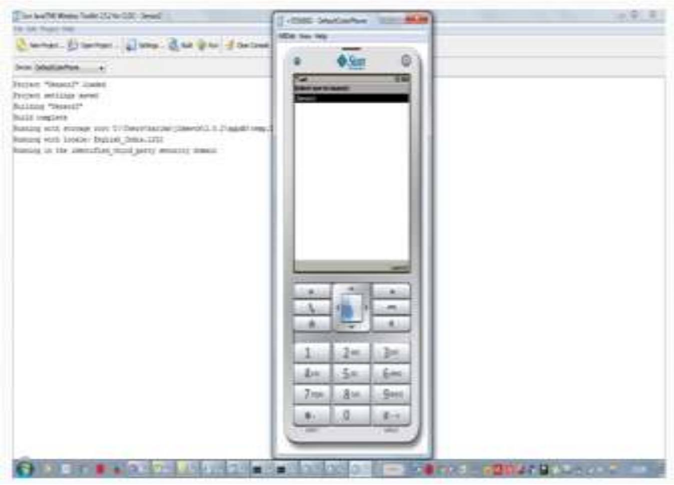
Build the process element(proc) and other sensors where proc is the main module which sends or receives the data from the sensors



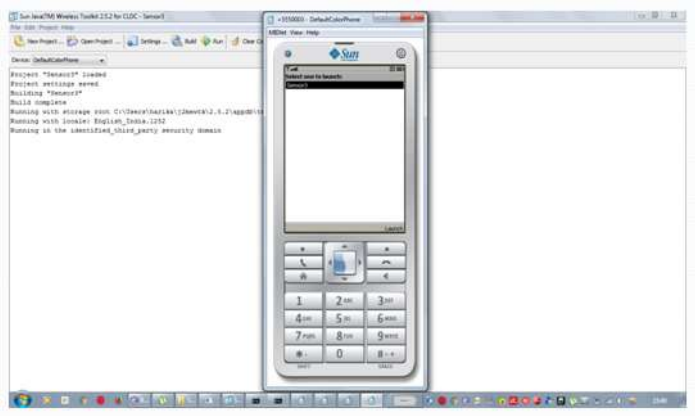
```
Project "Sensor1" loaded
Project settings saved
Building "Sensor1"
Build complete
Running with storage root C:\Users\harika\j2mewtk\2.5.2\
Running with locale: English_India.1252
Running in the identified_third_party security domain
```



```
Project "ProcElem" loaded
Project settings saved
Building "ProcElem"
Build complete
Running with storage root C:\Users\harika\j2mewtk\2.5.2\appdb\DefaultColorPhone
Running with locale: English_India.1252
Running in the identified_third_party security domain
```

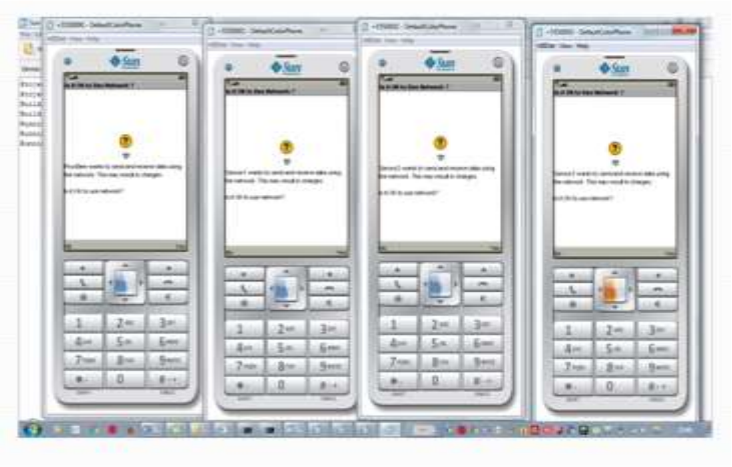


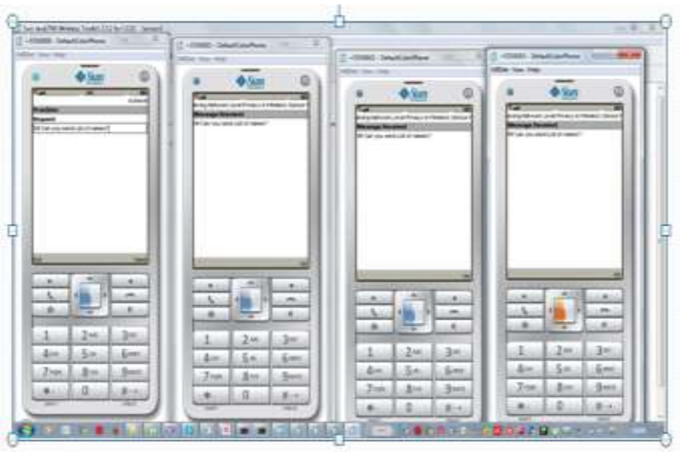
```
Project "Sensor2" loaded
Project settings saved
Building "Sensor2"
Build complete
Running with storage root C:\Users\harika\j2mewtk\2.5.2\appdb\temp.
Running with locale: English_India.1252
Running in the identified_third_party security domain
```



```
Project "Sensor3" loaded
Project settings saved
Building "Sensor3"
Build complete
Running with storage root C:\Users\harika\j2mewtk\2.5.2\appdb\t
Running with locale: English_India.1252
Running in the identified_third_party security domain
```

All the three sensors are synchronized with the proc element and hence a safe data transmission takes place





6. Conclusion

Existing privacy schemes of WSNs only provides partial network level privacy. Providing full network level privacy is a critical and challenging issue due to the constraints imposed by the sensor nodes (e.g.,energy, memory and computation power), sensor network (e.g., mobility and topology) and QoS issues (e.g., packet reach-ability and timeliness).

Therefore, in this paper we proposed a new identity, route and location based algorithm and how to integrate data successfully among the sensor nodes from a base or link node using wireless toolkit.

7. References

1. Xi, Y.; Schwiebert, L.; Shi, W. Preserving Source Location Privacy in Monitoring-Based Wireless

DOI: 10.18535/ijecs/v6i4.57

Sensor Networks. In *Proceedings of Parallel and Distributed Processing Symposium (IPDPS 2006)*, Rhodes Island, Greece, 2006.

2. Habitat monitoring on Great Duck Island (Maine, USA), 2002. Available online: http://ucberkeley. citris-uc.org/research/projects/great duck island (accessed on 21 August, 2009).
3. Ozturk, C.; Zhang, Y.; Trappe, W. Source-Location Privacy in Energy-Constrained Sensor Network Routing. In *Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks*, Washington, DC, WA, USA, 2004; pp. 88–93.
4. Kamat, P.; Zhang, Y.; Trappe, W.; Ozturk, C. Enhancing Source-Location Privacy in Sensor Network Routing. In *Proceedings of the 25th IEEE International conference on Distributed Computing Systems*, Columbus, OH, USA, 2005; pp. 599–608.
5. Misra, S.; Xue, G. Efficient Anonymity Schemes for Clustered
6. Wireless Sensor Networks. *Int. J. Sens. Netw.* 2006, *1*, 50–63.
7. Wood, A.D.; Fang, L.; Stankovic, J.A.; He, T. SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks. In *Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, VA, USA, 2006; pp. 35–48.
8. Ouyang, Y.; Le, Z.; Chen, G.; Ford, J.; Makedon, F. Entrapping Adversaries for Source Protection in Sensor Networks. In *Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06)*, Niagara-Falls, Buffalo, NY, USA, 2006; pp. 23–34.
9. Zorzi, M.; Rao, R.R. Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance. *IEEE Tran. Mob. Comput.* 2003, *2*, 337–348.