J. Sci. Trans. Environ. Technov. 2008, 1(4): 178-185

WATS-SNADSC: A Wireless Asset Tracking System using Sensor Networks with Auto Detect Spy Camera in Forensic Science

V. Veluchandhar* and K. Kandavel

*Department of Computer Science, St. Joseph's College, Tiruchirappalli - 620 002, Tamil Nadu, India.
Department of Biotechnology, Sengamala Thayaar Educational Trust Women's College, Sundarakkottai, Mannargudi - 614 001, India

Abstract

We present an asset tracking and early warning system against thefts called "Wireless Asset Tracking System using Sensor Networks with Auto Detect Spy Camera (WFTS-SNADSC)". This system uses concepts of Wireless Sensor Networks to detect a probable theft of an asset. The key objectives of the system are based on the typical characteristics of the environment where WATS-SNADSC has to operate. Overall architecture of the system is given followed by a detailed MAC layer design for the system. The system is designed so as to give warning in case a protected asset is removed from its designated area. The design takes care of situations where the sensors can be removed from the asset or an attempt is made to disable the system itself. The design is made to minimise the battery consumption of the sensors. The WFTS-SNADSC is implemented in a simulated environment to verify that the design meets all the key objectives of the system.

Keywords : WITTS-SNADSC, wireless tracking system, sensor networks, asset tracking, theft detection, forensics

INTRODUCTION

Theft has become a problem for all kinds of organisations globally. Due to easy movement and high resale value, digital equipments have always been prime targets of the thieves. In India 3,81,654 incidences of property crimes were reported during year 2000, which constituted 21.6 percent of total reported Indian Penal Code (IPC) crimes (Anonymous, 2001). All over the world larceny or theft crimes account for a significant portion of all the crimes committed. Billions of dollars are lost every year due to larceny crimes. Hence the government need a robust and effective asset tracking and theft warning system.

In this paper we present an architecture of how wireless sensor networks can be used for asset tracking and protection. Sensor networks comprise a large number of low-cost miniaturized computers each acting autonomously and equipped with short-range wireless communication, limited processing and memory, and a physical sensing capability. One of the most important parts of a wireless sensor network is the communication between the nodes. Sensor networks differ considerably from current networked and embedded systems. They combine the large scale and distributed nature of networked systems such as the Internet with the extreme energy constraints and physically coupled nature of embedded control systems (Callaway, 2003; Tubaishat and Madria, 2003).

Wireless Sensor Network applications include surveillance or security applications, asset tracking (e.g. Railroad cars or cargo containers), supply chain management, military applications, protecting property, health monitoring, monitoring of natural habitats and ecosystems, (Szewezyk *et al.,* 2004) environment observation and forecasting, home automation, intelligent agriculture etc.

Wireless sensor networks have been used to track nuclear materials in the Authenticated Tracking and Monitoring System (ATMS). ATMS uses wireless sensors, GPS receiver and the International Maritime Satellite (INMARSAT) (Callaway, 2003). Such a model cannot be employed to protect the assets of educational or research institutes as the cost of the system may be too high to be afforded by such organisations.

WATS-SNADSC is an affordable yet effective asset tracking and theft detection system. It works by attaching a low price sensor, called Infrared Sensor (IS) with spy camera, to each tracking point that is to be protected. A number of low price generic sensors are available today for this purpose. Although the price for a low end sensor is a few dollar at present; but it is expect that, with re-engineering, Moore's Law (Moore, 1965) and volume production the price of sensor motes can drop to a few cents in next several years . WFTS-SNADSC provides limited scalability in the form of that more area can be tracked by creating more segments, each containing a base station. We would like to keep the number of tracking points in a sensor network from low to moderate in order to get a quick response in case of asset tracking.

Earlier approaches for asset tracking and theft detection involve cable locks, motion detectors and other wireless approaches like RFID (Jae *et al.,* 2001). Cable locks and motion detectors have a draw back that they can be removed physically. In RFID approach RFID tags are affixed to each asset, we put limited range RFID readers at exit points . This can only detect theft if the asset is passed through these exit points. Also in RFID there is

*Corresponding Author
email: ***kandiyerphd@gmail.com***

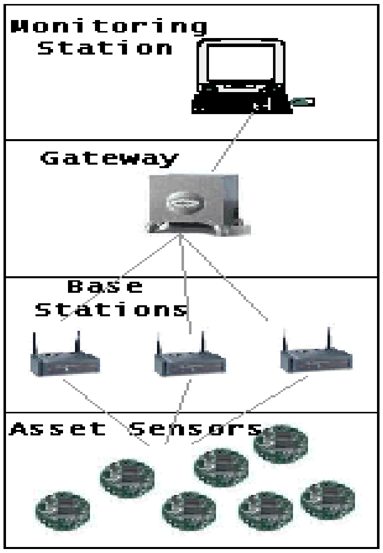


Figure 1. WATS-SN Architecture

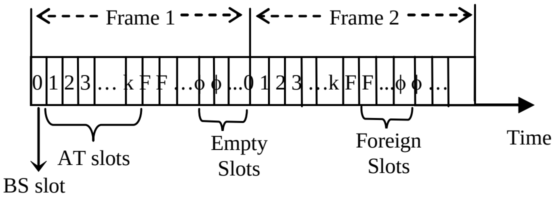
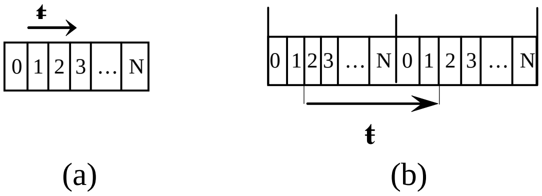


Figure 2. Division of time into frames and slots.



(a) (b)

Figure 3. Affect of the ordering of SIDs on massage latency

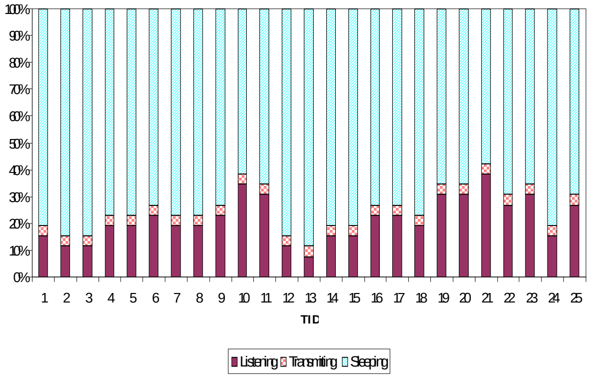


Figure 4. Sleeping behaviour of Asset Sensors

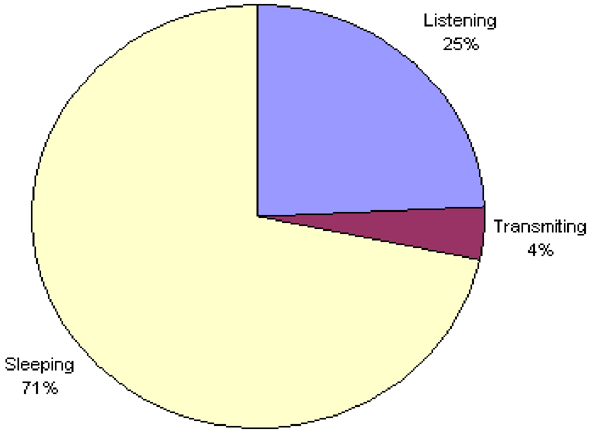


Figure 5. Average Sleeping Behaviour

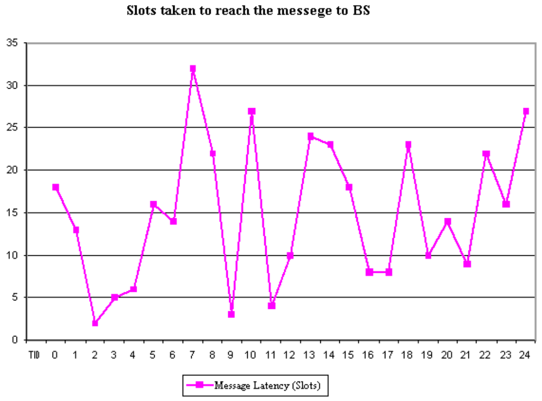


Figure 6. Message latency for simulated theft

no inter tag communication so tags cannot check the status of other nodes in their proximity.

Another feature of WATS-SNADSC is the Media Access control (MAC) design. A wealth of research has been done on design of MAC for Sensor networks (Bharghavan, *et al.,* 1994; Ye *et al.,* 2002; Kalidindi *et al.,* 2003). The MAC design affects the reliability, latency and energy consumption of the system. A study has been done in (Ye *et al.,* 2002) that has identified main sources of inefficiency for the RF medium and developed a solution based on PAMAS (Ye and Heidemann, 2003).

WATS-SNADSC is required to route messages from Asset Tags to the Gateway (GW). A lot of routing mechanisms are proposed as in (Heinzelman *et al.,* 1999; Zhang and Cheng, 2003; Zhao *et al.,* 2003) but all these mechanisms suffer from being too complex and involve lot of overhead. So we are using a simple routing mechanism based on flood routing.

SYSTEM SPECIFICATION

The following is the ideal operating environment for the system, system specification and goals, the assumptions.

Analysis and Assumptions

1. Each sensor network cluster for this application consists of moderate number of assets to protect. It is assumed that addition of new assets do not increase the diameter of the cluster[1] too much, instead the new asset can be joined in a new cluster. Further it is observed that assets usually are clustered in an area like Computer Laboratories have number of such assets placed together.
2. The time required for the initial set up of the network can be long but considering the long operational life of the system, this time is insignificant.
3. The network may not be operational during the maintenance or set up period.
4. As the assets are very costly so the investment in the system is justified.
5. There are two types of assets-non-mobile or fixed assets and semi-mobile assets requiring limited mobility. WATS-SN can be used for both.
6. The base station will be powered directly from the main supply. As a result the base station can have long range. Hence we assume that the Base Station can reach all the nodes in that cluster directly.

System Objective

WATS-SNADSC is a sensor network supposed to detect the motion of the object from a designated area and give signal to the spy camera for tacking video about the moving object. Then the sensor network node is relaying the video to the network administrator or security personnel. The WATS-SNADSC system warns when any of the alert condition has happened. The main system goals are as:

1. The WATS-SNADSC system must detect the moving object that alert condition has occurred.
2. The system must be able to route the information to the Base Station and ultimately to the Gateway.
3. The battery life should be maximised or in other words the asset sensors should have a low duty cycle.
4. The system should have provision of expansion by means of adding new tracking points to the existing clusters or creating new clusters.
5. Optional coordination with the Automatic Door Locking System can be done.

ARCHITECTURE

WATS-SN Architecture

The WFTS-SNADSC system consist of Infrared Sensors (IS) with Spy Camera, Base Stations (BS) and the Gateway. The architecture of the system has three layers as shown in Fig. 1.

The bottom layer has tiny inexpensive sensors with spy camera. The middle layer consists of all the base stations, controlling the asset sensors in a cluster. At the top layer is a Gateway, which is used, as an interface to the other existing networks. The monitoring station is a system on the LAN used to control and monitor the system.

In our approach the forest is divided in to number of geographical segments or clusters. Each cluster contains a moderate number of tracking points to trace and a Base Station (BS) that controls the Sensors attached to each of the tracking point. Each BS is in turn connected with the Gateway. The network decides that a theft is happening based on occurring of the alert conditions as given in section 3.2.

Infrared Motion detect Sensor with spy camera: The tracking sensor is a small sensor chip, which has a tiny processor, small amount of ram and flash memory and also includes a radio transceiver. It has many functions to perform. The first one is to transmit signal containing the status of the asset. It has to support the protocol given later in this paper. Another major function of the sensor is to detect its removal from the tracking point. There are many ways of achieving this functionality but these can be broadly categorised in to using the optical sensor, using resistive strip and using a mechanical button.

In the first approach the optical sensor is put beneath the Asset sensor. In case the asset sensor is removed from the asset, the light photons reach the optical sensor beneath it. So the sensor starts giving the ALERT messages.

In the second approach the sensor is connected through

[1] Cluster is defined in section 3.1.

a thin resistive strip, which forms an electric circuit running through the asset, sensor and the resistive strip. In case of removal of sensor from the asset, the circuit is broken and the sensor starts transmitting the Alert signal. The use of mechanical button is similar to its use in fire detection system where the button is situated behind a glass in pressed state. The glass has the words "Break glass in case if fire" itched on it. If the glass is broken, the switch is released resulting in to firing of fire alarm. In WATS-SN, the switch is between the sensor and the asset in a pressed state. As soon as the sensor is removed from the asset, the switch is released and starts transmitting the Alert signal. Design of the above switches is out of scope of this paper.

Each Asset Sensor is assigned a unique identifier called Sensor ID (SID). The SID is divided in to two parts Cluster ID (CID) and Local Sensor Number (LSN). The CID uniquely identifies cluster with in the whole set-up and LSN uniquely identifies an AS with in a cluster.

The Base Station: the BS has three major tasks to perform. First, it acts as a controller of its cluster in the sensor network. Secondly, it acts as a neighbour for other sensor nodes in its vicinity. Its third function is to communicate with the Gateway for this purpose it has a LAN interface.

The Gateway: Gateway is the central aggregation point for the whole network. It requires higher processing power and memory. It coordinates the whole sensor network. It can also, optionally, send automatic alert through email or text message. It is connected to a monitoring station that is maintained by the security personnel or administrator. In case of alert this monitoring station turns a siren on.

Alert conditions

The following scenarios can arise giving rise to different types of alerts. Each alert is given a different alert code because each alert is to be dealt differently.

Alert AC1 (Human Crossed): In case the human is crossed the tracking point. The neighbours notice this and raise an alert. This situation is represented by generating alert code AC1.

Alert AC2 (Sensor Removed): The sensor may be removed the sensor and leaving it behind. In this case the AS detects that it has been detached from the asset and alerts neighbours. This situation is reported by alert code AC2.

Alert AC3 (Base station unreachable or damaged): The BS may be disconnected from the power source or the link between the GW and the BS can be broken. In this case the GW does not hear any 'I am alive' message from the BS so it sends alert code AC3 to alert the network operator.

Alert AC4 (Gateway disconnected): The Gateway can be disconnected. In this case the system must send some alert message to the administrator. This is achieved by making a monitoring station sending the alert AC4.

Alert AC5 (Foreign AS in some sensor network): if an asset is stolen with AS still intact and it comes with in the range of some other sensor network, then the removed AS transmits a message (AC5) in one of the foreign slots with its SID in it .On hearing this message that foreign network will report to the GW that the stolen asset is currently in its range. This message is also sent to the gateway using the same code AC5. The BS mentions it SID also in addition to the SID of stolen asset. Note that in this case the alert is raised only if alert AC1 has been already raised in some other sensor network.

The Physical Medium

The Radio Frequency (RF) will be used for between the AS→AS and AS → BS communication. The existing network cables may be used for BS→GW communication. One of the problems with RF is Hidden Node or Exposed Node (Bharghavan *et al.*, 1994; Ye and Heidemann, 2003). This occurs when the topology is not known in advance. Decision regarding carrier frequency, modulation and de-modulation techniques to be used have to be made. However these topics are out of scope of this paper.

Media Access Control (MAC)

The WFTS-SN MAC design can be divided into two parts; first part for the AS ⇔ BS communication, second, is for the BS ⇔ GW communication. In the later case any of the existing LAN standards such as Ethernet or IEEE 802.11 wireless LAN standard etc. can be used. These are widely implemented and well established standards. We work to have a suitable MAC design for the first part. It must address the hidden node problem (Durst *et al.*, 2003) so as to achieve minimum latency in the ALERT messages so the alerts can be generated in a reasonable time.

Another major goal is to have maximum battery life. In the study done by Ye *et al.* (2002) there are four main sources of energy waste. The first one is collision. When a packet is corrupted it has to be discarded; the resulting retransmission will lead to more energy waste. Collision increases latency as well. The second one is overhearing, meaning a node picks packets that are destined for others. Third source is control packet overhead. The last major source is idle listening i.e. listening to receive possible traffic that has not been sent. The idle:receive ratio is measured from 1:2 (Kasten, 2002)to 1:1.05 (Stemm and Katz, 1997). According to (Ye *et al.,* 2002) idle listening alone can consume 50% - 100% of the energy required to actually receiving the message. Having a low duty cycle can control it.

In WATS-SN MAC design we try to control all the above-mentioned sources responsible for the wastage of energy. Mainly two approaches are used for Wireless Sensor Network MAC design, first the Contention Based approach, secondly the TDMA Based approach. In contention-based protocols, each node performs a carrier sense operation prior to transmission. If the channel is clear, the node can transmit. If the channel is not clear then node will have to re-sense the channel based on the protocol employed. This may avoid collision but it induces unnecessary delay (due to wait) that in turn may result in to a false alarm in case the BS is not able to hear "I am alive" message from an AS with in specified amount of time. It increases the duty cycle of the asset tag too. It requires the transmission of control packets to avoid collision e.g. CTS and RTS packets in 802.11 protocol (IEEE, 1999). This approach introduces three sources of energy wastage, idle listening, collision and control packet overhead. So this approach is not suitable for WATS-SN.

It is proposed to use the TDMA (Time Division Multiple Access) approach for WFTS-SN AS⇔BS communication. Considering the sources of inefficiencies brought out by SMAC (Ye *et al.,* 2002) we have used a solution based on SMAC and PAMAS (Singh and Raghavendra, 1999). DE-MAC (Ye *et al.,* 2002) also exploits the features of TDMA to prevent energy wastage by avoiding collisions and control packet overhead. In WFAT-SN we use a non-adaptive approach i.e. periodicity of transmission is not changed for a weak node. In this approach, time is divided into number of frames of equal interval (say τ). This frame in turn is divided in to a number of slots (say N) of equal duration (say τ). The number N is chosen by taking in to consideration number of ASs to be covered by the given network (say κ) and reserving few slots for nodes, belonging to some other cluster, that have been removed (unauthorised) and are currently with in the range of this network (see Fig. 2). Few empty slots may also be added so as to increase the sleep time there by decreasing the power consumption. Only one node can transmit in one slot. So all ASs get the right to transmit over the medium for a small time quantum in a round robin fashion.

TDMA also has its own disadvantages. One is initial set-up time, which is usually more because each node needs to know in advance when it has to transmit. Another problem is clock drift. This is due to crystal inaccuracy, which is caused by unavoidable reasons such as temperature change or aging etc (Venkatraman, 2004). In order to avoid clock drift the slots need to be longer or more frequent synchronization messages need to be sent. In our case however the disadvantages can be easily overcome.

In WATS_SN the slots are assigned to each node by BS and allocation is fixed i.e. slot for a particular node is not changed till the re-initialisation of the network. The slots are assigned on the basis of the LSN (Local Sensor Number) part of the SID, a unique identifier for any asset tag with in its sensor network. The Asset tag with LSN equal to 1 will transmit in slot number 1; LSN 2 will transmit in slot 2 and so on. The slot 0 is reserved for the base station. This scheme is simple because it does not have any overhead associated with the automation of this function and it is viable because new nodes are added or removed rarely. In case of addition of removal of new asset, that particular network is to be reinitialised. In this approach there is predictable latency, as the transmission time of each node is known in advance.

Inter-node communication

BS →AS communication

As we have assumed that the base station is powered from the wall so it can emit high power signals hence it can reach all ASs directly. Thus simplifying the initial set-up phase.

The slot 0 is assigned to Base station, this solves the clock drift problem. All ASs will synchronize their clocks to the beginning of the slot 0 which is also the beginning of the frame. So clocks are resynchronised after each frame this do not allow enough drift for an AS to start transmitting in other AS's slot.

AS → BS communication

Each AS in the system is required to transmit many messages to the BS however due to limited range of the AS and the fact that some devices may be put far away from BS such that the BS may not be directly reachable from some AS. In this case the message must be routed through some other AS. In our design each AS is required to forward message it heard in slots other than slot 0. As AS can transmit only in its allocated slot this forwarding must be done in that slot only. With this protocol the arrangement of the ASs too has effect on the time it takes to deliver message to the BS.

Consider two ASs with LSN numbers 1 and 2 are there in a Local Network L1, we assume that BS cannot hear AS with LSN 1 but can hear AS with LSN 2, further both ASs can hear each other. Now AS 1 transmits some message in slot 1. AS 2 hears it and retransmit it in slot 2 i.e. next slot. This way the massage reaches to the BS just 1 slot after it was sent (represented by t in fig. 3 a). Now consider the reverse scenario, i.e. BS can hear AS 1 but not AS 2. In this case AS2 transmits in slot 2 and AS1 hears it. Now AS1 can retransmit this message in slot 1 only, which will come in next frame. Assuming the number of slots is N, the time it has taken to reach the message is equal to N-1 slots (Fig. 3 b). So we see that the latency varies as the arrangement of the ASs changes.

To accommodate the mobility of the ASs we have to mark that asset as checked out by sending a special check out message. The Base station sends this message. After this message, its neighbour ASs won't expect to listen any " I am alive" message from that AS. Also it will be made sure that removal of this does not result in to the network being a disconnected graph.

BS ⇔ GW communication

As already discussed the communication between Base Station and Gateway is done using the current IEEE LAN standards like Ethernet or IEEE 802.11 wireless LAN standard etc. These standards use contention-based protocols at MAC level. This leg of the communication is also required to give messages with in certain maximum latency. But as the bandwidth for these standards is quiet high as compared with our need, we assume that this portion will not be the bottleneck for our purpose. So we can use the existing standard as it is.

PHASES OF OPERATION

Voting Phase

This is the initial set up phase. When all ASs are initially deployed, they all are in the state of idle listening. All the ASs listen for the BS to start transmitting and tell the start of the frame so that all ASs can synchronise their clocks with it.

The following events constitute the voting phase

1. The BS send a info message which contains the no of slots in a frame, duration of time frame, slot duration etc. This information is fed to the base station during the set up or installation by the administrator. ASs can determine the start time of each frame based on reception of this message.
2. Next the base station sends the Status Request (STR) message in slot 0. After receiving the STR message each AS sends the STA message in its assigned slot. The STA message contains the information about the battery remaining. It also serves as "I am alive" message.
3. Third step involves preparing of neighbour list. In this step each AS listens to each slot and if it hears any transmission in this slot then it will add this slot in its neighbour list. Similarly BS also prepares its neighbour list.
4. In this step the administrator may do the network connectivity check. If the digraph representing the network is connected then it is a connected network. The BS issues a Send Neighbour List (SNL) message. Each AS then responds with a Neighbour List Response (NLR) message, which contains the neighbour list. This step is optional.

The neighbour list may be too big to be transmitted in single slot. In this case the message may be fragmented, the AS, in this case, sends the number of messages to follow. This information can be used to adjust power setting of the ASs so as to maximise the battery life.

The BS sends the STD message to let the ASs enter in to standard operation mode

Standard Operation Phase

During Standard Operation the BS sends the SYNC message in slot 0. Upon receiving this message all ASs resynchronise their clocks. Each AS will wake up only in the slots corresponding to other ASs which are in its neighbour list (to listen) and in its own slot to transmit. During other slots it will be in sleep mode. BS and GW are never in sleep mode. The Base Station and Gateway exchange Status Message (STA) after a fixed periodic interval. To perform the AS addition, AS removal and maintenance operation the Administrator will send the reset (RST) message.

Mobility: As we mentioned that WATS-SNADSC can be used for assets with limited mobility (semi Mobile). To enable an asset to move out of the network (with authorization of course) there is provision to mark a node to be out of the network (Logically) so that no alarms are caused due to removal of this asset. For this purpose we have a provision of Asset Check-out (ACO) and Asset Check-in (ACI) messages.

When an Asset is to be moved out of network, the BS issues an ACO message specifying the SID of the asset. On hearing a ACO message each AS in the network checks the SID in the message. If it is its own SID then it assumes that it is no longer in the network. This AS does not send any STA messages now onwards. It waits for the ACI message so that it can rejoin the network. This AS listens for slot 0 and resynchronise it every time. If the SID is of one of the ASs in its neighbour list then it doesn't expect any STA message from that AS.

When the asset that was earlier taken out is again required to join the network, the BS broadcasts an ACI message containing a SID. Each AS receives this message. If for any particular AS this message contains SID of an AS that was previously in its neighbour list then it will start to expect STA messages from it. If the message contains its own SID then it starts sending STA messages now onwards.

Alert Mode

During the Standard Operation mode each AS expects STA message from its neighbours in their respective slots. If any AT does not send STA message then it assumes that It has been, in an unauthorised way, moved out of its location (or possibly been stolen). So it will generate an ALERT message (AC1) and transmit in its slot. ALERT message can be triggered by other situations also as already explained in section 3.2.

At this point there is a transition from Standard Mode to Alert Mode. During alert mode only ALERT messages are being transmitted. Each mode will transmit ALERT message it heard from its neighbour. It is like Flood Routing. The BS will ultimately get this ALERT message and it passes this to the GW, which in turn informs other Base Stations in the WATS-SN Set up. We will explain how the system handles each scenario.

Scenario 1: In this scenario (AC1) lets assume that node AS3 has been removed by some unauthorised person and it has a neighbour AS5, further AS5 can reach BS directly but AS3 cannot. The neighbour (AS5), after observing that they are not getting any STA message from AS3, sends AC1 message to BS. The BS then sends message to GW informing the SID of the stolen asset. The Gateway alerts the Administrator about the incident. The administrator can take the required action as per the policy of the organisation. Which may include automatically closing the exit doors or sounding a siren or warning security persons etc. The gateway alerts other Base stations too about the theft. Each AS in the whole system starts listening to the foreign slots also in addition to the slots in their neighbour lists. At this moment the system is ready to track the asset.

Suppose the stolen AS has reached in the range of some sensor network controlled by other BS. As all ASs in this SN are aware of the theft, they are listening to the foreign slot also. Now this asset will come to know about the slot number of foreign slots from the Slot 0 transmission by the BS (say Slot 7 through 9). It will send an alert (AC5) containing its SID in any slot out of these three slots. Any node, which is in the range of this stolen node, will hear the Message and it transmits another AC5 alert in its designated slot. Eventually the alert will reach its BS, which in turn will inform the GW. In this way, the movement of the stolen asset can be tracked.

Scenario 2: In this scenario the asset is stolen but the tag is detached from the asset and left in its original location. In this case the AS on the asset being stolen will come to know about the fact that AS has been detached. It transmits an alert message in its next designated slot with its SID and alert code AC2. This alert will eventually reach the BS and then to the GW. In this case there is no need to alert other sensor networks about the theft as the AS is lying at original location itself so it can not transmits alert messages in the foreign sensor networks. The GW alerts the administrator or any other integrated systems.

Scenario 3: In this scenario the BS is disconnected from its power source or the link between the BS and GW is broken. In this case the GW does not hear ant keep alive message from the BS so it warns the monitoring workstation or the administrator.

Scenario 4: In this scenario the GW itself is disconnected so it cannot warn the administrator. So the monitoring workstation will hear no information from BS so it has to send warning message to the administrator.

The ALERT can be passed to the security System of the organisation or some email or text message may be sent to the Security in-charge or administrator. The detail of how a message or email is sent is out of the scope of this paper.

When the cause of the alert is known and handled, the administrator may send a RST message through the BS. All nodes again come in to the Voting Phase.

SIMULATION RESULTS

We have implemented WATS-SN in a simulation environment by writing specialised C++ application and using the Visual Sense simulation framework for wireless and sensor networks included in Ptolemy II (Baldwin *et al.,* 2004). We simulated the system by taking IDRBT (Institute of Development for Research in Banking Technology) as the test case. IDRBT has around 400 computers located at its 2 buildings. Here we have given the results of simulation of the Executive Development Centre (EDC) lab situated at the 3rd floor of EFC building at the IDRBT campus, which has 25 computers and also houses the central office of the Indian Financial Network (INFINET). The EDC lab is formed in a single cluster with a base station and 25 asset sensors. The neighbour list after the Voting Phase is shown in Table 1.

Table 1. The Neighbour list of a cluster after voting phase

Node	Neighbour List
BS	{1,2,3,4,5,9,10,14,15,21,22}
1	{2,3,4,12}
2	{1,3,4}
3	{1,2,4}
4	{1,2,3,5,9}
5	{4,6,9,10,22}
6	{5,7,9,10,11,21}
7	{6,8,10,11,23}
8	{7.11.19.23.24}
9	{4,5,6,10,21,22}
10	{2,5,6,7,9,11,19,20,22}
11	{6,7,8,10,19,20,21,23}
12	{1,13,14}
13	{12,14}
14	{12,13,15,22}
15	{14,16,21,22}
16	{11,15,17,20,21,22}
17	{16,18,19,21,22,25}
18	{17,19,20,23,25}
19	{8,11,17,18,20,23,24,25}
20	{10,11,16,17,18,19,21,23}
21	{6,9,10,11,15,16,17,19,20,22}
22	{5,9,10,14,15,16,21}
23	{7,8,11,18,19,20,24,25}
24	{8,19,23,25}
25	{17,18,19,23,24}

Fig. 4 shows the sleeping behaviour of each node. It shows the percentage of time that a node spent in sleeping, transmitting and listening. The fig. 5 gives the overall view of fig. 4. It shows the average behaviour of each node. We can see that on average each node sleeps for 71 % of time. However there is a trade off between sleep time and response time or latency. If we increase the range of the sensors so that each AS has more neighbours then the latency will decrease but the nodes will be awake for more time, resulting in more battery consumption. So we can tune the sensors as per our need.

We have also simulated theft of each node. As we have already discussed the response time also depends on the time of theft. The time of theft is based on a randomly chosen number. The message latency[2] for each node in the simulation is given by the Fig. 6.

CONCLUSION

In this paper we presented WATS-SN, an asset tracking and early warning system against thefts, using wireless sensor networks. The system is designed using a layered architecture that includes asset sensors, base stations and a gateway.

The WATS-SNADSC system gives a design that has the basic features for any theft detection and warning system. Still there is a lot of scope for improvement. The WATS-SNADSC system uses a non-adaptive transmission scheme for the sensors. If we have a mechanism to have the sensors transmit using variable power depending on their individual status such as battery remaining then the false alerts, caused due to drained battery, can be reduced.

REFERENCES

Anonymous, 2002. Crimes in India 2001, National Crimes Records Bureau, New Delhi, India, 2002, http://www.ncrb.nic.in.

Baldwin, P. and Kohli, S. Edward A. Lee, Xiaojun Liu, and Yang Zhao. 2004. Modeling of Sensor Nets in Ptolemy II, *In:* Proceedings of Information Processing in Sensor Networks, (IPSN), April 26-27, 2004, Berkeley, CA, USA.

Bharghavan, V., Demers, A. Shenker, S. Zhang, L. 1994. Macaw: A media Access Protocol for Wireless LANs, Proceedings of the ACM SIG-COMM Conference, London Aug. 31-Sep. 2, P. 212-225.

Callaway, E.H. Jr. 2003. Wireless Sensor Networks, Auerbach Publications, New York.

Durst, R.C. and Grace, K.H. 2003. Mobile Ad Hoc Networking for Transformed Army, The MITRE Corporation, Bedford, USA.

Heinzelman, W.R., Joanna Kulik, Hari Balakrishnan. 1999. Adaptive protocols for information dissemination in wireless sensor networks, *In:* Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking 1999 (MobiCom '99) Seattle, Washington, United States, August 15 - 19, 1999, P. 174-181.

IEEE, 1999. LAN MAN standards committee of IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks", IEEE Standard 802.11 [ISO/IEC 8802-11] New York, USA, 1999.

Jae, S.K., Quershi Anique A. and Siegel Joel G. 2001. The International Handbook of Computer Security, Glenlake Publishing Company Ltd., Chicago.

Kalidindi, R., Ray, L., Kannan, R. and Iyengar, S. 2003. Distributed Energy Aware MAC Layer Protocol For Wireless Sensor Networks ICWN 2003, Las Vegas, Nevada, USA.

Kasten, O. 2002. Energy Consumption, http://www.inf.ethz.ch/˜kasten/research/bathtub/energy_consumption.html, Eldgenossische Technische Hochschule Zurich.

Moore, G.E. 1965. Cramming More Components Onto Integrated Circuits, *Electronics*, 38(8): 114-117.

Singh, S. and Raghavendra, C. 1999. PAMAS: Power Aware Multi-Access protocol with Signalling for Ad Hoc Networks. *ACM Computer Communications Review,* 28: 5-26..

Stemm, M. and Katz, R.H. 1997. Measuring and Reducing Energy Consumption of Network Interfaces in Hand-Held Devices, IEICE Transactions on Communications, Vol. E80-B, no.8, P. 1125-31.

Szewczyk R., Osterweill E.J., Polestre M. Hamilton A. 2004. Mainwaring and D. Estrin, Habitat monitoring with Sensor Networks, *Communications of the ACM*, June 2004, Vol. 47(6): 34-40.

Tubaishat, M. and Madria, S. 2003. Sensor Networks: An Overview", *IEEE Potentials*, Vol.22(2): 20-23.

Ventakataraman, L. 2004. Design Trade-offs in Wireless Sensor Network System Development, Robert Bosch Corporation, Palo Alto, CA, USA.

Ye, W. John Heidemann, and Deborah Estrin, 2003. An Energy-Efficient MAC Protocol for Wireless Sensor Networks, *In:* Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), 23-27, June 2002, New York P. 1567-1576.

Ye, W., John Heidemann, 2003. Medium Access Control in Wireless Sensor Networks USC/ISI Technical Report, ISI-TR-580, Information Science Institute, California, USA, October 2003, http://www.isi.edu/~weiye/pub/isi-tr-580.pdf.

Zhang, Y., Liang Cheng, 2003. Self-nominating: A Robust Affordable Routing for Wireless Sensor Network, *In:* Proceedings IEEE Vehicular Technology Conference 6-9 Oct. 2003 (VTC 2003), Orlando, USA, 2003, Vol. 5: 2828-2833.

Zhao, S., Tepe, K., Seskar, I. and Raychaudhuri, D. 2003. Routing Protocols for Self-Organizing Hierarchical Ad-Hoc Wireless Networks Proceedings of the IEEE Sarnoff Symposium , Princeton, NJ.

Erratum:

In this paper following error were published.

1. Abbrevations WFTS-SNADSC and WITTS-SNADSC should read as WATS-SNADSC in all places.

2. Abbrevation WFTS-SN MAC should read as WATS-SN MAC in all places.

3. Abbrevations WFTS-SN and WATS-SN should read as WATS-SN in all places.

4. Author name in citation at page no. 178 should be Szewczyk et al., 2004 not Szewezyk et al., 2004.

5. In Reference section the author name Ventakataraman, L. should read as Venkatraman, L.

[2] The message latency is given in number of time slots taken to reach the message to Base Station.