Asian Journal of Information Technology 6 (12): 1200-1204, 2007
ISSN: 1682-3915

Implementation of Bluetooth Sensor Security Network Through SCTP

[1]R. Kanthavel, [2]L. Ganesan and [3]R. Dhaya
[1]Department of ECE, Government College of Engineering, Tirunelveli, India
[2]Department of Computer Science and Engineering, A.C. Technology, Karaikudi, Tamilnadu, India
[3]Department of Information Technology, National Engineering College, Kovilpatti, Tamilnadu, India

Abstract: The advancement in wireless communication does meet many challenges like flexibility and mobility of nodes in a Network apart from cost effectiveness. Particularly in the wired network, the sensor nodes tend to undergo unnecessary congestions in the way of communication, while it uses Transport Control Protocol (TCP). Moreover low response from one node to another node, poor self configuration of network and routing in Bluetooth wireless network demands an alternative protocol that must get rid of the difficulties. So here the proposed Bluetooth sensor network utilizes the SCTP (Stream Control Transmission Protocol) in order to improve the efficiency and our simulated output shows the good variation from the existing network.

Key words: SCTP, TCP, sensor nodes, bluetooth wireless network, communication, congestion

INTRODUCTION

The Bluetooth wireless sensor network using TCP, the important problems monitored are the lack of reliability among nodes in the view of exchanging information, conjestion of path. So it is best and better for a node to have more than one address for avoiding conjestion between two nodes and also the efficiency of the Bluetooth wireless sensor network can be improved a lot when a sequenced delivery of data involved between nodes. In this proposed study, the advantages of SCTP have been taken to improve the efficiency of Bluetooth wireless sensor network by means of creating primary path and secondary path for a single node.

Existing problem: In the existing wired sensor network system since all the nodes have to be connected by wires, whenever they are setup, wires must link the sensor nodes. Moreover, the position of the sensor nodes cannot be changed that results lack of intelligence. In addition with that using Transmission Control Protocol (TCP) suffers from 'Head of the line' blocking and restrictive congestion control mechanisms which lead less reliability and poor flexibility (Kamal *et al*., 2005) among nodes while the information exchanges. If a node contains more than one address then the other node can easily contact even a particular path is congested and TCP does not have the provision to create more than one address for a single node. The sequenced delivery of user messages within multiple streams, with an option for order of arrival delivery of individual user messages is also not possible while using TCP. Thus the efficiency of Bluetooth sensor network can be increased by means of using Stream Control Transmission Protocol (SCTP).

Proposed network: The proposed network comprises sensor nodes, relay nodes and a control node. All the nodes have been interconnected with each other through Bluetooth module. Sensor node is capable of sensing the signal which may be treated as unwanted one. The received signal is then to be conveyed to control node through relay node. Here relay node is nothing but as the router and once the information reaches over the control node an acknowledgement does come via this relay node to the sensor node. All the three kinds of nodes transmit and receive packets via a Bluetooth model, that is embedded in them (Fig. 1 and 2).

The three basic security services defined by the Bluetooth specifications are as the following:

Authentication: A goal of Bluetooth is the identity verification of communicating devices. This security service addresses the question "Do I know with whom I'm communicating? This service provides an abort mechanism (Rodzevski, 2004) if a device cannot authenticate properly.

Confidentiality: Confidentiality, or privacy, is another security goal of Bluetooth. The indent is to prevent information comprise caused by eavesdropping (passive attack). This service, in general, addresses the question Are only authorized devices allowed to view my data?

Corresponding Author: R. Kanthavel, Department of ECE, Government College of Engineering, Tirunelveli, India

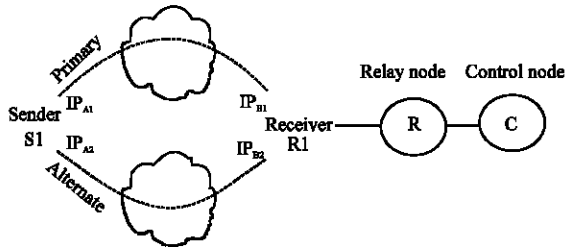

Fig. 1: System overview

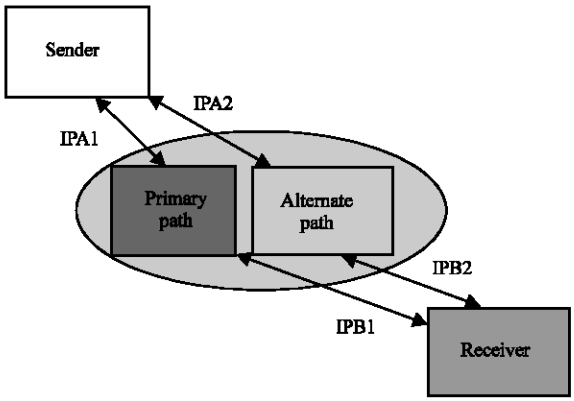

Fig. 2: Proposed network

Authorization: A third goal of Bluetooth is a security service developed to allow the control of resources. This service addresses the question "Has this device been authorized to use this service.

The characteristics of Bluetooth technology are as follows:

- Each Bluetooth model is a 9mm *9 mm tiny chip.
- Upto three voice channels.
- Data protection: authentication, Encryption with 8…128 bit key.
- Power consumption: about 30 mA.
- Frequency: 2.4 GHz (ISM range).
- Distance : 10 m (There are solution for 100 m as well).
- Data rate.
  - Asymmetric mode: 721/57.6 Kbits/sec.
  - Symmetric mode: 432.6 Kbits/sec both ways.

Fundamental differences between TCP and SCTP: SCTP uses Streams to transmit data, which are appropriate for message-based applications. This differs from TCP's byte-stream method, which delivers a stream of bytes in the same order as it was presented by the application. SCTP is more sophisticated and the data can be divided up into different streams. Each stream can then be delivered with its own characteristics and largely independent from other streams. Streams can be defined as' Strictly-Ordered and Reliable', like TCP, or just 'Reliable', so that data will be delivered to the application as soon as it arrives. The Head-of-Queue Blocking of TCP, which prevents it delivering subsequent data if data is lost, is avoided as each stream operates independently. SCTP can deliver data to the application while waiting for the retransmitted Protocol Data Unit (PDU) to be delivered.

The second difference relates to the way SCTP interacts with the IP layer. TCP assumes that each host has only one IP address, while SCTP introduces the possibility that many different IP addresses are possible. For any transport protocol, it is important to be able to identify the source of incoming information. SCTP allows an association to use a range of available IP addresses, so that it is possible to have (n) × (m) pairs of valid IP addresses, where n and m are the number of available IP addresses at each end-point. The main reason for doing this is to make an association more resilient to network failures, since the signaling community expects a higher level of reliability than is generally available from the network.

NECESSITY OF SCTP

SCTP is a Reliable Transport operating on top of a connectionless packet network such as IP that offers congestion avoidance behavior providing the feature of multihoming that enables SCTP end points to support multiple IP addresses. Multihoming protects an association from potential network failures by steering traffic to alternate IP addresses therefore each end point can send and receive from any of the IP addresses listed at the remote end point. In the existing TCP loss of session could be triggered by core network failures or by isolation of end points. In the other hand, the sequenced delivery of user messages with in multiple streams is also possible in SCTP, which is not in TCP.

Streams in SCTP: TCP delivers data in the same order as the data is presented to it. Therefore, if a PDU is not delivered in sequence, or gets lost, TCP will not deliver subsequent PDU until the lost one is successfully delivered. If a link fails, this leads to head-of-queue blocking, where the performance of the connection suffers while waiting for the lost PDU (Stewar *et al*., 2000; Zou *et al*., 2006). If the application is not concerned about in-order delivery then this additional delay is unnecessary. For instance, if a device is a router, it might be in the process of synchronizing stored statistics with a database.

During this, if an interface fails, the Network Administrator needs to be informed of this as soon as possible. It is not sufficient that this warning is queued behind the synchronization data. SCTP overcomes this by assigning it a separate stream, so that the warning is delivered as soon as it arrives, without unnecessary delays caused by sharing the association with the synchronization.

In order to facilitate streams and some other features of SCTP, the notion of chunks is introduced. As opposed to the TCP byte-stream, information in SCTP is segmented into chunks, which are then carried inside an SCTP PDU. It is the chunks that are acknowledged using a scheme based on the TCP option of Selective Acknowledgements (SACKs) (Fig. 3).

Multi-homing in SCTP: As mentioned previously, a significant difference between TCP and SCTP is that SCTP does not limit an association to the same two IP addresses for the duration of the association. This raises many interesting issues, some of which are discussed here. During association initialization, each end-point of the potential SCTP association advertises any IP addresses that are available to it. This allows the end-points to create a list of addresses. They must then accept any PDU's with a valid address pair for the duration of the association. In order to ensure validity, port number and verification tag are also included with each PDU. SCTP does not use the multiple links for load sharing, though there is nothing in the standard that specifically rules this option out. It operates by designating one of the addresses of the Corresponding end-points as the Primary Address and will attempt to communicate with this address, while all other addresses are Secondary Addresse (Yih-Chun and Perrig, 2004). It does not specify any particular IP address as a source address, but instead allows the operating system to decide. In the case of an error, it will retransmit the chunk to a secondary address. This is different from TCP, as TCP requires a connection to maintain the same addresses for the duration of the connection (Shaojian and Atiquzzaman, 2003). IP routing at an end-point can affect SCTP redundancy. If each end of the association has two interfaces, each with an IP address, then the operating system might decide that the best way to reach either peer address is via the same local interface. If that interface develops a fault, then the entire association may collapse.

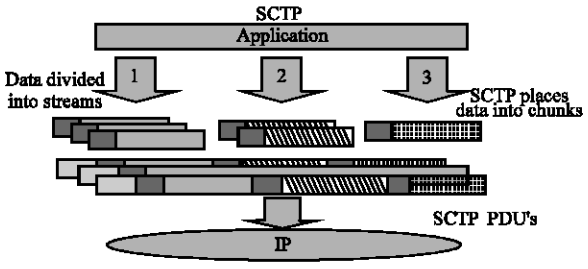

Fig. 3: SCTP data delivery

OPERATION OF PROPOSED BLUETOOTH SENSOR NODES

The Bluetooth technology has the features like, the devices can be networked, the signals can be transmitted through walls thus eliminating the need for line of sight, (Joe, 2003) the separation of frequency band into hops where spread spectrum technique is used that adds a strong layer of security, omni-directional signals, support of synchronous and asynchronous applications and standardization in usage of Bluetooth technology. The Fig. 4 illustrates the Bluetooth stack.

The operations related to the events are summarized as follows:

External input event: We simulate this event by means of the on-off switch. the node detecting this event makes a message packet corresponding to the event for reporting it to the local.

Security control system: To send the packet, it searches the logical address of its parent node from the address table and then pages the parent node to send the packet.

Retransmission time out events: These events are further classified into the transmission timeout for the link level ARQ and the retransmission output for the upper layer ARQ.

Inquiry time out event: This event occurs when the timer for periodic inquiry timeouts.

Paging event: This event happens when a node is paged.

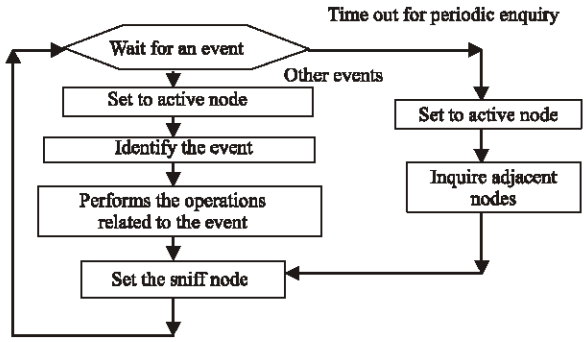

Fig. 4: Operating flow chart

RESULTS

The simulation of the proposed Bluetooth wireless sensor network has been done using TCP as well as SCTP. The simulation results shows that the enquiry time and exchange time are significantly and reasonably found to be less in SCTP rather than TCP. Moreover, the reliability of the proposed network increases and the overall security level can also be improved while using the SCTP resulting a congestion free network (Fig. 5).

At first experiment of the proposed network starts Relay node 6 to Relay node 5 data transmission (Fig. 6).

After completing the node 5 to node 6 transmission, the Relay node 5 data is transmitted to Relay node 2 (Fig. 7). The above two steps are over then the data is transmitted to relay node 2 to control node 1 (Fig. 8).

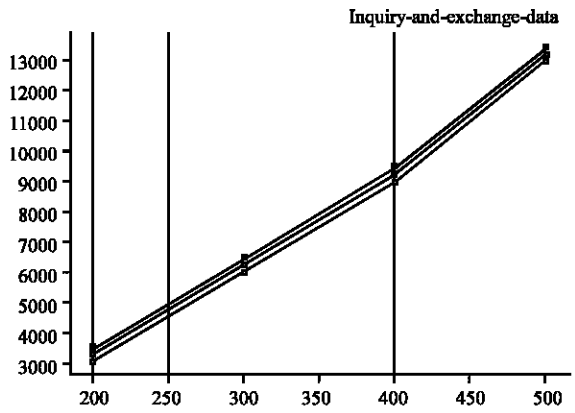

Fig. 5: Inquiry and exchange time for STCP and TCP

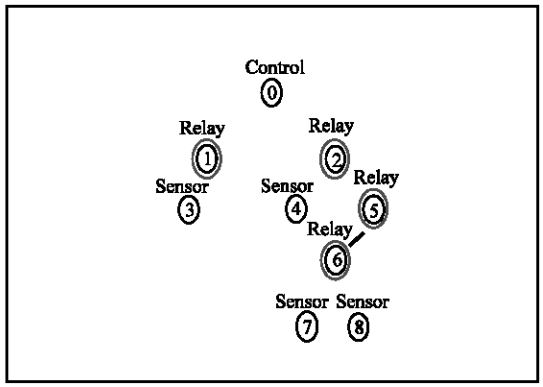

Fig. 6: Node 6 to 5 transmission

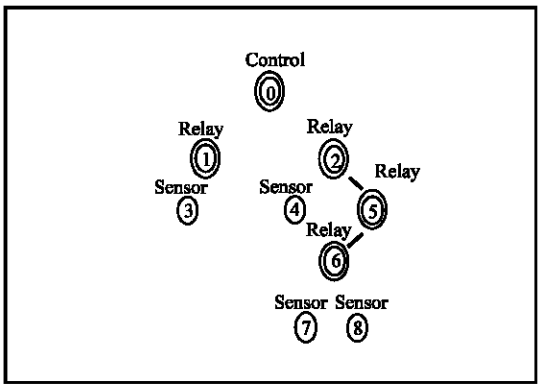

Fig. 7: Node 5 to 2 transmission

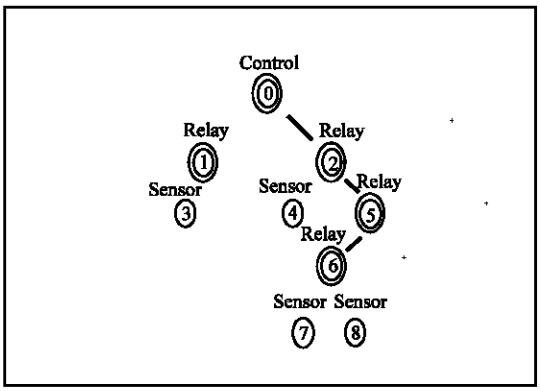

Fig. 8: Node 2 to 0 transmission

CONCLUSION

Taking the advantages of small size, low power consumption and low cost from Bluetooth technology together with the merits of SCTP in the way of multistreaming and multihoming the outputs have been studied. Our simulation results infer that the number of nodes, inquiry and exchange of data with transmission time are comparatively reduced while using SCTP in Bluetooth wireless sensor network for security.

REFERENCES

Alexander Rodzevski, 2001. Creating a Wireless Sensor Network using Bluetooth Technology. TR-TS-765.

Joe, I., 2003. SCTP with an improved cookie mechanism for mobile ad-hoc networks. Global Telcommun. Conf. GLOBECOM, IEEE ., 7: 3678-3682.

Kamal, H., B. Penoff and A Wagner, 2005. SCTP versus TCP for MPI, Supercomputing. Proc. ACM/IEEE SC Conf., pp: 30-30.

Shaojian Fu and M. Atiquzzaman, 2003. Improving end-to-end throughput of Mobile IP using SCTP. High Performance Switching and Routing, HPSR. Workshop, pp: 171-176.

Stewar, R. and Q. Xie *et al*., 2000. RFC 2960: Stream Control Transmission Protocol. The Internet Society.

Yih-Chun Hu and A. Perrig, 2004. A survey of secure Wireless Ad-hoc Routing. IEEE. Security and Privacy, 2: 28-39.

Zou, J., M.U. Uyar, M.A. Fecko and Samtani, 2006. SF-SCTP: An Extension of Stream Control Transmission Protocol to Support QoS. Networking, Sensing and Control. ICNSC. Proc. IEEE. Int. Conf., pp: 780-785.