Journal of King Saud University – Computer and Information Sciences (2017) **29**, 449–461

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

An Efficient Route Maintenance Protocol for Dynamic Bluetooth Networks

Sabeen Tahir [a,b,*], Sheikh Tahir Bakhsh [a], Abdulrahman H. Altalhi [a]

[a] *Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Makkah, Saudi Arabia*
[b] *Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia*

Received 13 April 2016; revised 28 July 2016; accepted 28 July 2016
Available online 1 August 2016

KEYWORDS

Bluetooth network;
Route maintenance;
Weak links;
Prediction;
Backup device

Abstract Bluetooth is a widespread technology for small wireless networks that permits Bluetooth devices to construct a multi-hop network called scatternet. Routing in multi-hop dynamic Bluetooth network, where a number of masters and bridges exist creates technical hitches. It is observed that frequent link disconnections and a new route construction consume extra system resources that degrade the whole network performance. Therefore, in this paper an Efficient Route Maintenance Protocol for Dynamic Bluetooth Networks (ERMP) is proposed that repairs the weak routing paths based on the prediction of weak links and weak devices. The ERMP predicts the weak links through the signal strength and weak devices through low energy levels. During the main route construction, routing masters and bridges keep the information of the Fall Back Devices (FBDs) for route maintenance. On the prediction of a weak link, the ERMP activates an alternate link, on the other hand, for a weak device it activates the FBD. The proposed ERMP is compared with some existing closely related protocols, and the simulation results show that the proposed ERMP successfully recovers the weak paths and improves the system performance.

1. Introduction

Bluetooth specification is designed for the low power two-way radio communication to connect the network devices over short distances (Chih-Min and Yin-Bin, 2014). The Bluetooth physical layer operates on the 2.4 GHz Industry Scientific and Medical (ISM) frequency band. The key advantage of the ISM frequency band is that it makes the Bluetooth technology accepted worldwide (Laharotte et al., 2015). A Bluetooth device can play the role of a master, slave or bridge. A Bluetooth basic networking unit is called a piconet which behaves like a cluster in an ad-hoc network topology that contains the maximum of eight Bluetooth active devices out of 256 devices.

* Corresponding author at: Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Makkah, Saudi Arabia.
E-mail addresses: stsheikh@kau.edu.sa (S. Tahir), stbakhsh@kau.edu.sa (S.T. Bakhsh), ahaltalhi@kau.edu.sa (A.H. Altalhi).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2016.07.003
1319-1578 © 2016 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

In a piconet, one Bluetooth device becomes a cluster head known as a master device and other devices become slaves. Within a piconet, direct slave to slave links are not allowed and all communicating links go through the master device. A master device treats the slave devices in a Round Robin (RR) fashion that basically overcomes the collision between devices (Singh and Agrawal, 2011).

To decrease the interference between devices, Bluetooth technology uses the Frequency-Hopping Spread Spectrum (FHSS) Jin-Ho et al., 2014; Subhan et al., 2012 technique. The use of FHSS makes the Bluetooth technology less susceptible to signal congestion and eavesdropping than other wireless technologies. Each Bluetooth device uses 79 channels using a pseudo-random hopping sequence. Each Bluetooth device uses a running clock, and all slave devices stay synchronized to the piconet from time to time adding a timing offset to their clocks from the clock of the master (Etxaniz and Aranguren, 2015). In a Bluetooth network, each active slave device is also allocated a 3-bit Active Member Address (AM_Addr) by the master device. Bluetooth devices discover each other and make the connections. Initially, all the devices are in standby mode only the native clock (CLKN) runs. The Bluetooth clock monitors the timing and hopping sequence of the transceiver, it is typically executed as a 28-bit wrap-around counter (Yu and Lin, 2012; Sharafeddine et al., 2012).

The master sends requests to the other Bluetooth devices to make a piconet. Devices which agree to make a piconet reply to the master's request. The master device sends the ID packets on different frequencies and waits for the reply packets called Frequency Hopping Sequence (FHS) packets from the slave devices. The device sends not only a FHS packet but also its ID and clock value. A Bluetooth device in the inquiry scan mode decreases its hopping frequency; this mode gives consent to the inquirer to catch up with the transmit frequency of the Bluetooth device which is in the inquiry scan mode (Ramana Reddy et al., 2010; Yu, 2010). As the frequencies match, the scanned devices behave like slave devices and transmit their ID and clock information to the master device. The time interval between the starting of two consecutive page scan operations is considered as the scan interval time, $T_{inquiry\_scan}$, that should be less than or equivalent to 2.56 s (Cui et al., 2010). When Bluetooth devices exceed more than eight devices, they make a scatternet (Subhan et al., 2011). A scatternet is a combination of interconnected piconets where a device of one piconet (master/slave) elects to contribute as a slave in other piconets. This intermediate device is called a bridge/relay device that relays the data between piconets. By using this approach, more interconnected piconets can make a large network (Xin and YuPing, 2009) as shown in Fig. 1.

There are many Bluetooth multi-hop routing protocols which have been proposed for inter-piconet communication, but it has been analyzed that none of them consider the route breakage issue (Bo et al., 2012; Yu, 2012; Aldabbagh et al., 2015a,b; Tahir and et al., 2013). Most of the researchers proposed ideas for route optimization without considering route breaking issues. It is true that if the main routing link breaks, it creates some serious problems like delay, unnecessary energy consumption, packet loss, etc. Therefore, it has provided an opportunity to propose an Efficient Route Maintenance Protocol for Dynamic Bluetooth Networks. The proposed protocol overcomes the problem of frequent link breakage and provides a solution in terms of predicting weak links.

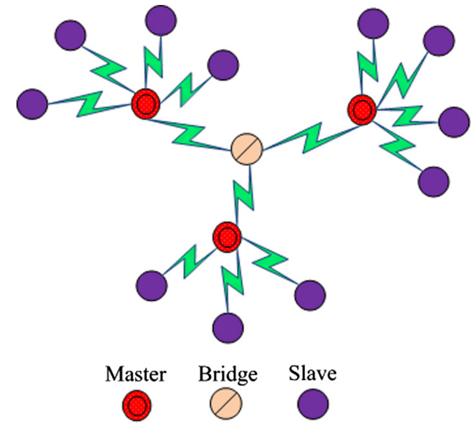

Figure 1 Bluetooth scatternet where one bridge device links three piconets.

The remaining portion of this paper is organized as follows. Section 2 discusses the related work of the proposed protocol. To overcome the frequent link breakage problem, the proposed protocol is presented in Section 3. The performance analysis of the proposed protocol and its comparison with a few similar protocols is shown via simulation in Section 4 using the NS-2 (The NS-2 Simulator, 2014) and UCBT (Agrawal and Wang, 2007). Finally, the conclusion and possible future work is presented in Section 5.

2. Background and related work

In a piconet, direct slave to slave communication is not possible so all communicating links (outgoing and incoming) data traffic go through the master device; therefore, the master is the most important device. If a master device goes down or moves, it may disconnect all linked devices. Similarly, within a scatternet, direct master to master communication is not possible as they always need an intermediate bridge device, therefore, the bridge device is considered as the most significant device because it connects multiple piconets (Ching-Fang and Shu-Ming, 2008). If it fails or moves, then it can disturb the whole network. When data are routed between two Bluetooth networks for slave to slave communication, it follows the rule that the data will go through "slave-to-master – bridge-master-slave". Although, many researchers have proposed different ideas for routing and scatternet formation for a Bluetooth network, but in this research, we considered only the most relevant protocols.

The authors proposed a dynamic energy-aware network maintenance (DENM) protocol Bakhsh and et al., 2011, where a master device maintains a table storing all the connected slave devices' information. When the energy level of the master device reaches L_1, it activates an auxiliary master from its slave devices. Similarly, if a bridge device energy level reaches L_1, it sends a request message to the connected master devices for backup relay activation. This technique provides flexibility against frequent link discussion based on the energy level. The main drawback with this technique is that it does not consider device mobility which can cause frequent link disconnection. The DENM is explained through Fig. 2(a), where source device A transmits data to the destination device D passing

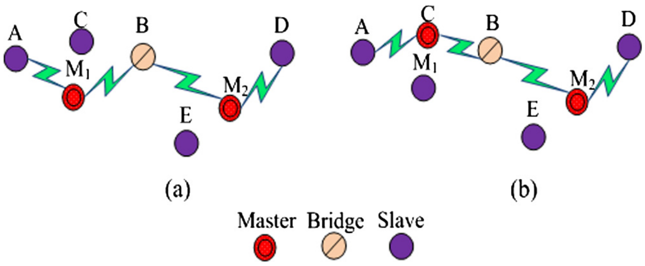

Figure 2 Route maintenance using DENM protocol.

through A–M_1–B–M_2–D. Once the energy level of M_1 reaches its limit, it activates C as a new master and starts transmission through the A–C–B–M_2–D route as shown in Fig. 2(b).

The second relevant protocol is the Novel Route Maintenance (ROMA) Sahoo et al., 2008 for Bluetooth ad-hoc networks. ROMA maintains a routing path for a Bluetooth scatternet. If devices are added or removed from the network, ROMA decreases the number of hops by adding new devices and reconstructs the routing path. In ROMA, if a new device joins or leaves the scatternet it maintains its routing link by considering the number of hops. The respective master device checks the new device to find out whether it can reduce the hop counts and make the routing path shorter; then, it changes the role of the new device and creates a new piconet(s) within the routing path. Although ROMA works well, it does not consider the change to the device's role once the communication has ended. Moreover, ROMA does not provide any solution in the routing path for the devices that want to communicate with their original master device or slave device in the network. According to ROMA, if a Bluetooth device moves away from the piconet, it informs its master device for the device leaving procedure which takes extra time and consumes more resources.

As an example shown in Fig. 3(a), source device A is transmitting data to the destination device D through routing path (A–M_1–B–C–D) and data are also routed from the source device E to H through the routing path (E–J–H). Fig. 3(b) shows that during data transmission, a new device I enters into the piconet M_1. M_1 is a routing master, it checks that this device can provide the shortest path. As device I and D are direct within the radio range of each other, the routing master breaks the existing link and makes the new link A–I–D. Meanwhile, device F starts moving and goes out from the range of the routing masters, M_2 and M_3. When it starts moving, it informs the routing masters so they can find another device J, that can re-establish the route E–J–H as device E is now transmitting data through a new route; however, if suddenly, device J fails due to energy level, it would not be able to inform its routing master. In the above scenario, ROMA fails to provide any solution to continue transmission. Therefore, this has provided an opportunity to propose a new protocol for route maintenance to overcome the inefficiencies of existing protocols.

BlueStar is a scatternet development technique, where each node, after the discovery stage, calculates its weight on the basis of its degree and other parameters, and compares them with its neighbors for determining its role as (master/ slave). The BlueStar protocol sets up its own separate piconets; a node that has a higher weight compared to its neighbors will become the master and the remaining nodes will become slaves. The master node selects a bridge node to connect with neighboring piconets. In the resultant BlueStar scatternet, each piconet can contain more than seven slave nodes. However, it is observed that having more than seven slave nodes in a piconet could degrade the performance.

Another scatternet protocol called BlueMesh (Emre and Oznur, 2006) has been proposed for the improvement of the BlueStar protocol. BlueMesh activates in two stages; in the first stage, it determines one and two hop neighboring nodes and in the second stage, the Bluetooth nodes select their roles. BlueMesh defines a procedure for handling the topology variations based on the insertion and removal of Bluetooth nodes. When a new node wants to join the scatternet, it first broadcasts identity packets and then the receiving nodes reply with a FHS packet. New nodes can receive FHS packets from more than one neighbor; in this case, a decision is required for connection establishment. It has been analyzed that BlueMesh's large control overhead is due to device role selection.

3. The proposed ERMP protocol

The proposed Efficient Route Maintenance Protocol for Dynamic Bluetooth Networks (ERMP) is discussed is this section. Bluetooth technology does not allow direct slave to slave or master to master communication in different piconets. Therefore, the Bluetooth devices need to follow the communication rules (slave-master) and (master-bridge-master). In the proposed ERMP, when a main link is established, each routing

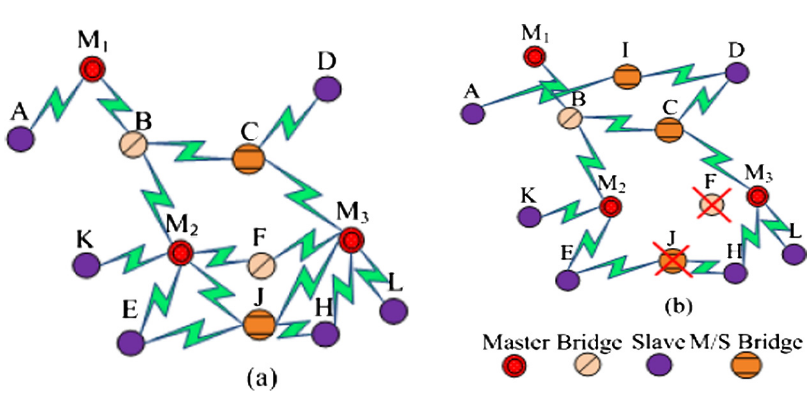

Figure 3 Routing problem in the ROMA scatternet.

master and routing bridge update their tables and save the fallback devices' information. During transmission, if a weak link or weak device is notified, the proposed protocol creates a new link to overcome the frequent link disconnection using fallback devices. When a fallback device is unavailable, the proposed protocol performs a role switch operation for route maintenance.

3.1. System model for a connected scatternet

Suppose N is the total number of Bluetooth devices (slaves, masters, and bridges) in a scatternet as follows.

$$N = S \cup M \cup B \tag{1}$$

$$P_i(S_{ij} \in M_i) = \begin{cases} 1 & S_{ij} \text{ connects } M_i \\ 0 & S_{ij} \text{ does not connect } M_i \end{cases} \tag{2}$$

$$\text{Subject to} \quad S_{ij} \leqslant 7, \forall i \tag{3}$$

$$\text{Distance } ED(S_{ij} \wedge M_i) < 10 \text{ m} \tag{4}$$

where S, M, and B denote the number of slaves, masters, and bridges, respectively. Where P_i is the ith piconet and M_i corresponds to the piconet master, S_{ij} is the jth slave device in the ith piconet. S_{ij} is set to 1 if there is a master–slave relationship between device i and device j, otherwise it is set to 0. Constraint (3) determines if each piconet (P) has the maximum seven slave devices and that the maximum distance between the master and slave devices is 10 m in constraint (4).

A connected scatternet has intermediate devices (bridge/relay) to provide communication in multiple piconets. Eq. (5) represents an intermediate device relay, where P_i and P_j are any two piconets and n_b is an intermediate device between these piconets.

$$P_i \cap P_j = n_b \quad \text{where } i \neq j \tag{5}$$

In each piconet, the routing master maintains a Routing Master Information Table (RMIT) that contains the list of slave devices, clock offset, device ID, device status (active/inactive), energy level, signal strength, FallBack Masters, and FallBack Bridges. On the other hand, in a scatternet, each routing bridge maintains a Routing Bridge Information Table (RBIT) that contains the list of connected master devices, device status (active/inactive), signal strength, energy level, FallBack Bridges, FallBack Masters and master's degree.

$$\text{Degree}\left(R_1^k, M_j\right) = \begin{cases} 1 \text{ for } R_1^k \text{ connected } m_j \\ \text{null } R_1^k \text{ no connection with } m_j \end{cases} \tag{6}$$

where R is a relay and k is the degree of relay, each relay with a connected master (M) has a value of 1 and null otherwise.

The flow diagram of the proposed ERMP is shown in Fig. 4, where three colors are used, the gray color shows that both master and slave execute these steps, while, dark colored steps represent a master device and lighter colored steps represent a slave device.

3.2. Route maintenance protocol

The proposed ERMP protocol is implemented in the dynamic Bluetooth network that forecasts the mobility of devices to improve the network stability, where devices can move any time with different speed and direction. Therefore, the Random Walk Mobility Model (RWMM) is used for the proposed protocol because it considers the speed and direction of the devices. RWMM is a simple mobility model based on the random directions and speeds from a predefined range (Kuo Hsing Chiang, 2004). The mobile device can move from its present position to a new position by randomly selecting the directions and speed. From Eq. (7), the time is divided into the time slots t = 0, 1, 2..., where at t = 0, the device can choose one of four adjacent units $\{(x + 1, y), (x - 1, y), (x, y + 1), (x, y - 1)\}$ with the same probability of 1/4. This procedure is repeated in every subsequent time period. The position of a device at timeslot t = 0, 1, 2... is denoted by $C_{(n)}$ (t) that basically shows the unit where the device exists.

$$(x, y), x, y \in \{0, 1, 2 \ldots n - 1\} \tag{7}$$

3.2.1. Mobility-base link replacement

Before starting communication, a routing link is established between intermediate devices, the device participating in the route are called routing devices. A routing link within a scatternet passes through multiple piconets; therefore, the routing link consists of several routing master devices. A piconet that holds the routing master device is known as the Bluetooth routing inter-piconet. Whenever a new device enters into the routing piconet it sends its complete information to the routing master. Each routing master and routing bridge device maintains their tables. The masters monitor routing devices Signal-to-Noise Ratio (SNR). The received power signal strength can be utilized to estimate the distance, as all the electromagnetic waves show the inverse square relationship between the distance and received power. The relationship between the distance and received power is as follows.

$$P_r \propto 1/d^2 \tag{8}$$

The received power between the transmitter and receiver is indicated by P_r and d is the distance.

During transmission, a weak link is notified if any intermediate device between any pair of source and destination starts moving. When an intermediate device starts moving away from a piconet the routing master observes its weak signal strength because the device is going out of radio range. Eqs. (9) and (10) are used for calculating signal strength.

$$PRe = PTr * GRe * GTr * (1/(4 * \tau * d))^2 \tag{9}$$

where PTr is transmit power, GRe is receiver antenna gain and GTr is transmitter antenna gain.

$$d = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \tag{10}$$

where d is the distance between the master and moving device and x and y are the current position of the devices.

In the proposed protocol, each routing master device maintains its table in which it keeps the information of the signal strength (from the master device to the connected slave device), device status, energy level, clock off-set and the role of the device (FallBack master, FallBack Bridge). The routing bridge device keeps the information of the device ID, device status, signal strength (from the bridge device to connected master devices), energy level and the role of the device (FallBack master, FallBack Bridge) in its table. A threshold ρ = −45 db is defined for the signal strength, which is fixed for all routing

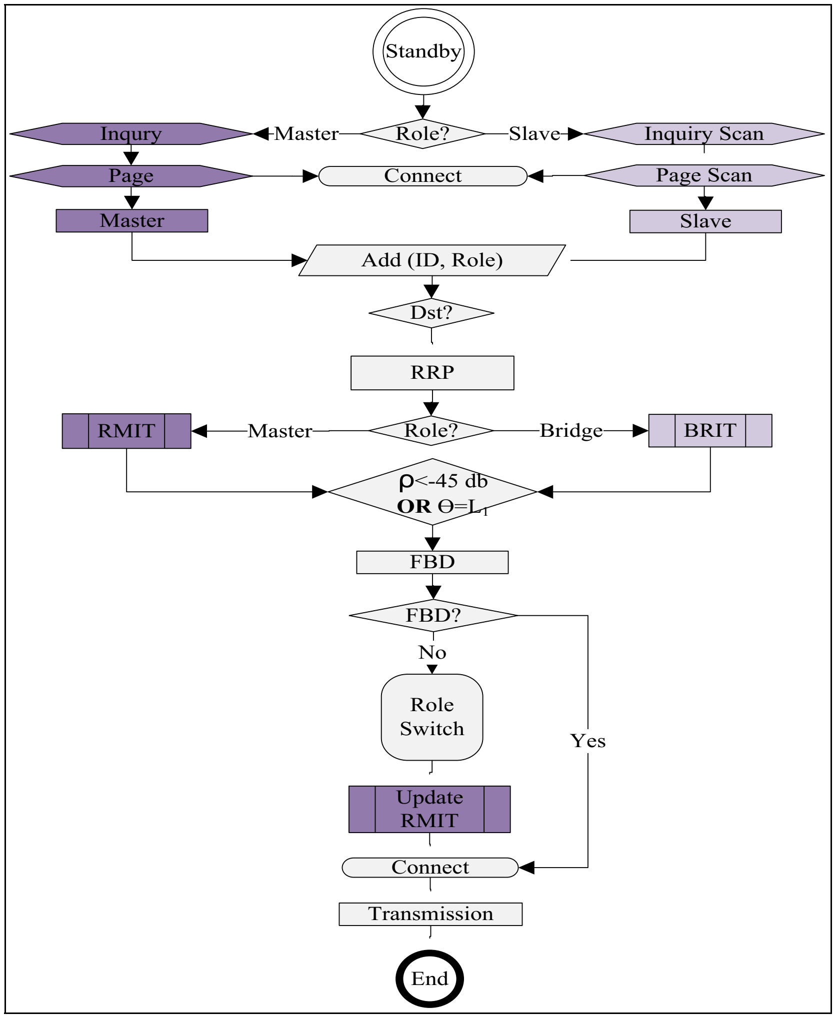

Figure 4 System flow diagram.

devices. If any intermediate device in a routing link starts moving, the signal strength between the routing master and the moving device gradually decreases. The routing master can easily predict a weak signal strength as the device is moving and it can choose an appropriate routing device to make a new link before the main route breaks. When a routing bridge device starts moving, the routing master device checks for a FallBack Device (FBD); the routing master device activates the FBD and maintains the routing link. If the FBD is not available, the routing master device chooses another device (that may be a slave device) and changes the role of the device as required. The master insures that the new device must be within the radio range of both the devices so it can maintain the routing link efficiently. A routing link between two directly connected devices is considered weak if the devices have a weak signal strength. Fig. 5 shows different links between two devices. Any routing device can be weak, slave, master, or bridge. If a device becomes weak multiple devices are available as FBDs, the highest priority is given to a bridge because it can connect multiple piconets. The second priority is given to a master as it can connect multiple slave devices within a piconet. A slave has the lowest priority due to its limited role in the network.

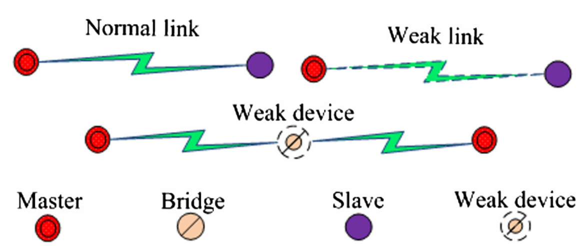

Figure 5 Different links between source and destination.

The proposed ERMP is explained through Fig. 6(a). The routing master M_3 stores the active devices' information in RMIT as listed in Table 1. On the other hand, B_2 is a routing bridge and stores connected master inform in RBIT as listed in Table 2. Source A and destination C are communicating through the route A–M_1–B_2–M_2–B_4–M_5–C and the second link is between source D and destination E which are communicating through the route D–M_4–B_3–M_2–B_6–M_3–E. During transmission between A and C, the bridge device B_2 starts moving upward, in the meanwhile the routing masters M_1 and M_2 predict that the bridge device B_2 is going out of range.

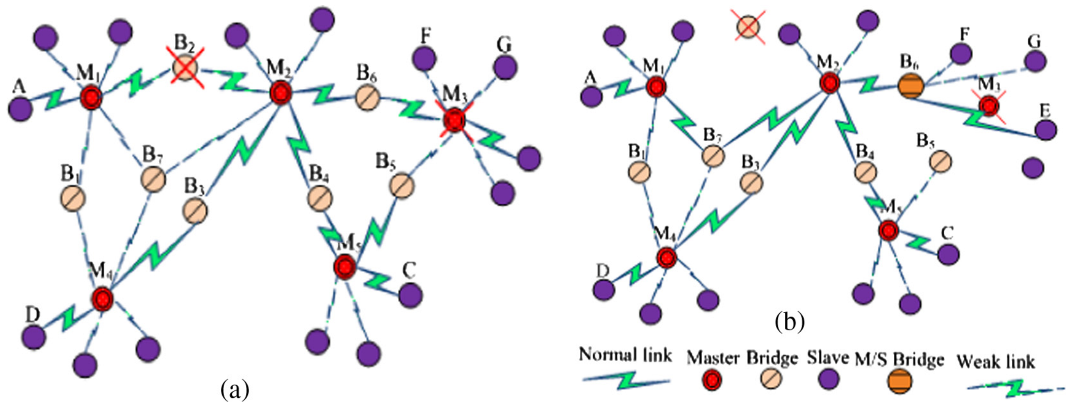

Figure 6 Before and after link replacement.

Table 1 Routing Master Information Table (RMIT) for M_3.

Device ID	Clock off-set	Device status (active/inactive)	Signal strength (dBm)	Energy level	Device role
E	c-offset(E)	Active	$S^t_{M3\text{-}E} = -70$	L_3	Slave
F	c-offset(F)	Inactive	$S^t_{M3\text{-}F} = -65$	L_2	Slave
G	c-offset(G)	Inactive	$S^t_{M3\text{-}G} = -76$	L_2	Slave
H	c-offset(H)	Inactive	$S^t_{M3\text{-}H} = -66$	L_3	Slave
B_5	c-offset(B_5)	Inactive	$S^t_{M3\text{-}B5} = -60$	L_1	Bridge
B_6	c-offset(B_6)	Active	$S^t_{M3\text{-}B6} = -60$	L_3	FBM (M/S bridge)

Table 2 Routing Bridge Information Table (RBIT) for B_2.

Device ID	Device status (active/in active)	Signal strength (dBm)	Energy level	Device role
M_1	Active	$S^t_{M1\text{-}B2} = -45$	L_2	Master
M_2	Active	$S^t_{M2\text{-}B2} = -50$	L_2	Master

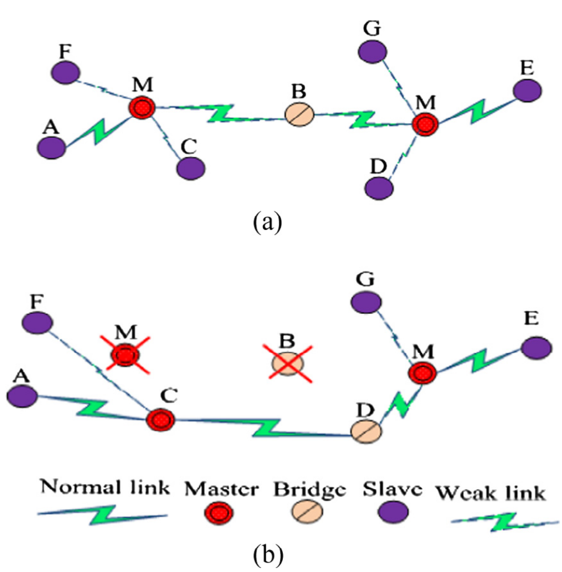

Figure 7 (a) Prediction of weak link and weak device. (b) Maintenance role switch operation.

Table 3 Simulation parameters.

Parameters	Values
Simulation area	80 m × 80 m
Number of devices	15–90
Number of pairs	84
Data packet type	DH3, DH5
Traffic model	CBR
Communication range	10 m
Energy consumption	0.0763×10^{-6} J/bit
Power class	B
Device deployment	Random deployment
Mobility model	Random Walk Mobility Model
Mobility speed	0.5–3.0 m/s
Polling algorithm	Round Robin
Bridge scheduling algorithm	MDRP
Packet size	100–500 bytes
Inquiry time	10.24 s
Page time	128–256 s
Packet interval	0.1–0.5 s
Queue length	50 packets
Simulation time	1000 s

The masters execute the device leaving procedure and find out which device can replace the weak link. As B_7 is a potential FBD, that can replace B_2, therefore, both masters execute the replacement procedure and transmit a request to B_7 to make a new link between M_1 and M_2.

The master M_1 transmits an ID packet along with a Device Access Code (DAC) repeatedly until it receives a response. The master M_1 does not know on which hop frequency B_7 will wake up so that is why it broadcasts a train of the same DACs on different hop frequencies and listens for a reply. The master M_1 utilizes the BD_Addr and the clock of the B_7 device to obtain the page hopping sequence. B_7 performs the page scan that is similar to the inquiry scan in which a Bluetooth device listens and replies. There exist 32 paging frequencies including a page hopping sequence which is obtained by the BD_Addr of the master. The B_7 changes listening frequencies after 1.28 s.

The master M_1 freezes its predictable B_7 clock to the value that triggered a reply from the paged device. It is equal to using the clock values estimation when receiving the B_7 response. The frozen clock value is used at the content where the recipient's access code is identified. Let N be a counter that starts from zero and increases by one for each time when $CLKN_1$ is set to zero which matches the start of a master TX slot. Finally, B_7 reconstructs the sub route by replacing the weak link. As shown in Fig. 6(b), the new link between M_1 and M_2 is established and the data will go through the new route.

3.2.2. Energy-base link replacement

University of Cincinnati Bluetooth (UCBT) presents four levels of energy, i.e., L_0, L_1, L_2 and L_3. The proposed ERMP defines a threshold (θ) value for the energy level. A device is called a weak device, if the energy level of any device gets to L_1. The master device selects a FBD to create a new link. During the route request each device includes its available battery level to the route request packet and forwards it to the next hop. This procedure carries on until the route request packet arrives at the final destination. Each master device calculates the master's average power MP_{avg} using Eqs. (11) or (12) as below:

$$MP_{avg} = \frac{i_{Tx} \times 1/2T_{sniff} + i_{Rx} \times 1/2T_{sniff}}{T_{sniff}} \times V \tag{11}$$

$$MP_{avg} = 1/2(i_{Tx} + i_{Rx}) \times V \tag{12}$$

where Tx and Rx are the transmission and receive slots. The voltage of the Bluetooth's specific chip is indicated by V and T_{sniff} is the sniff mode interval. The slave device's Rx and Tx average power is calculated as below:

$$SP_{Rx} = \frac{(N_{sniff\_attempt} \times t_{slot}) \times i_{Rx}}{T_{sniff}} \times V \tag{13}$$

$$SP_{Tx} = \frac{i_{Tx} \times t_{slot} + ((N_{sniff\_attempt} - 1) \times t_{slot}) \times i_{Tx\_idle}}{T_{sniff}} \times V \tag{14}$$

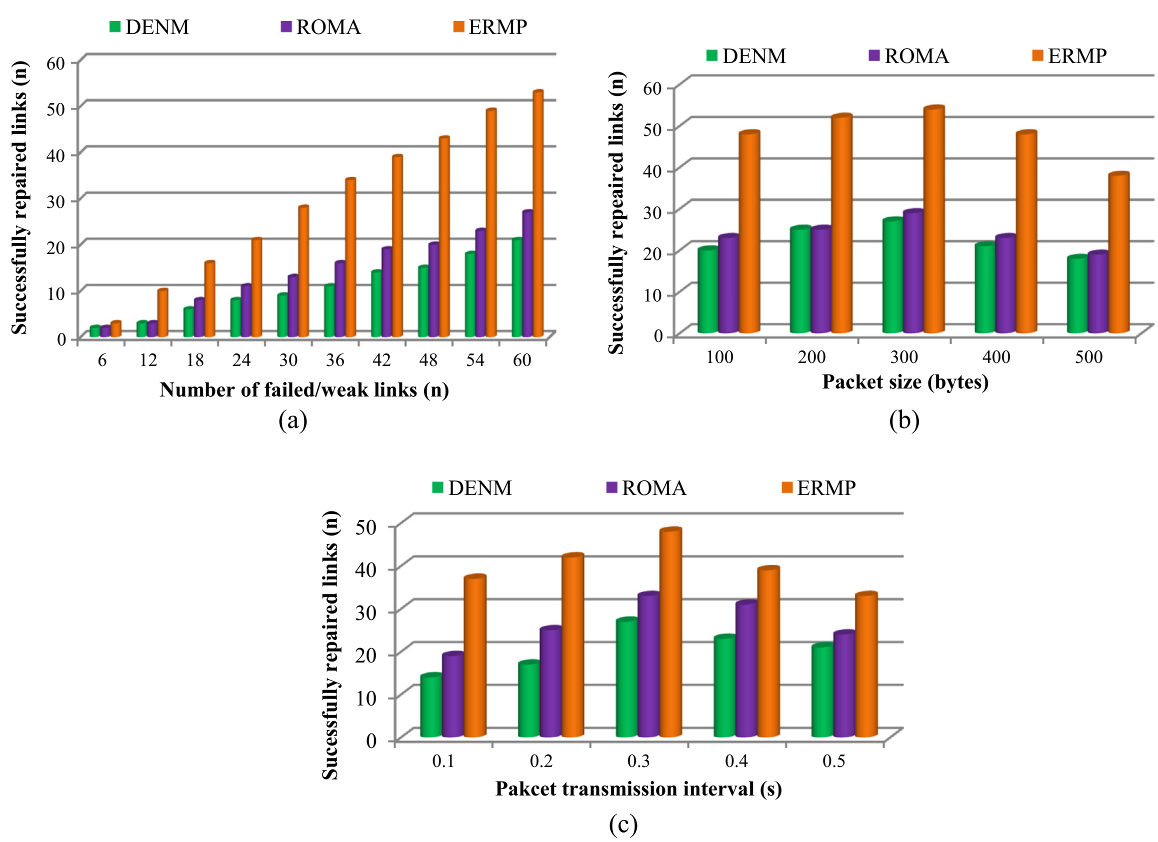

Figure 8 (a) Repaired links vs. number of failed/weak links. (b) Repaired links vs. packet size. (c) Repaired links vs. packet transmission interval.

where i_{Tx} is a task slave device when it transmits and i_{Tx_idle} is a task of a slave device when in idle mode or not transmitting.

The routing links are defined for the pairs of source and destination devices, where the source device initiates the route request for the destination device. The source device forwards a RSP to the master device and the master device forwards the received packet to the connected bridges. Once the destination device receives the RSP, it sends the unicast RRP to the source device. As the energy level of the intermediate routing device is gradually decreasing, when it reaches the specified limit L_1, the routing master updates its status as a weak device and chooses another appropriate FBD as given in Eq. (15). If data are forwarded from the bridge device to the weak master device and the master device has to forward the data to the slave or bridge device, then a weak master device will check if the next device is within the radio range of the bridge device or not. If the next device is within the radio range of the bridge device, the weak master device sends a request message to the bridge device to switch the role from bridge to master/slave bridge and make a direct link to the next device before the weak master device dies. Finally, the routing master activates a new link and forwards the data through the new link.

$$FBD = FBD_l \subseteq R_k \quad \text{where } l \text{ and } k \text{ represent the bridge degree (number of connections)} \tag{15}$$

As shown in Fig. 7(a), devices M_1 and M_2 predict that device B starts moving from its position and it is also predicted that the energy level of M_1 is gradually decreasing so the routing link between M_1 and M_2 becomes weak. In this case, when a master device itself becomes weak, it first of all finds a device that will become the master device; so, from its table, it selects device C and sends a request for the role switch operation from slave to master. Now, device C becomes a new master device so it updates its table. The master device C fines device D within its radio range and also within the range of $M_{2;}$ so, device D works as a bridge between these piconets. For route maintenance, devices C and D make new links. In Fig. 7(b), the new routing link is A-C-D-M_2-E and data go through the new route.

4. Simulation results and discussion

This section evaluates the simulation results by comparing numerous performance metrics: healing delay, control packet overhead, blocking connections, route recovery time and slot utilization. The proposed and base protocols implemented UCBT (Agrawal and Wang, 2007) based on The NS-2 Simulator, (2014). Table 3 shows the list of parameters (Sahoo et al., 2008) that were used in the simulation. The area of 80 m × 80 m was taken in which the Bluetooth devices were scattered randomly. The Bluetooth devices were varied between 15 and 90, and 84 pairs of source and destination

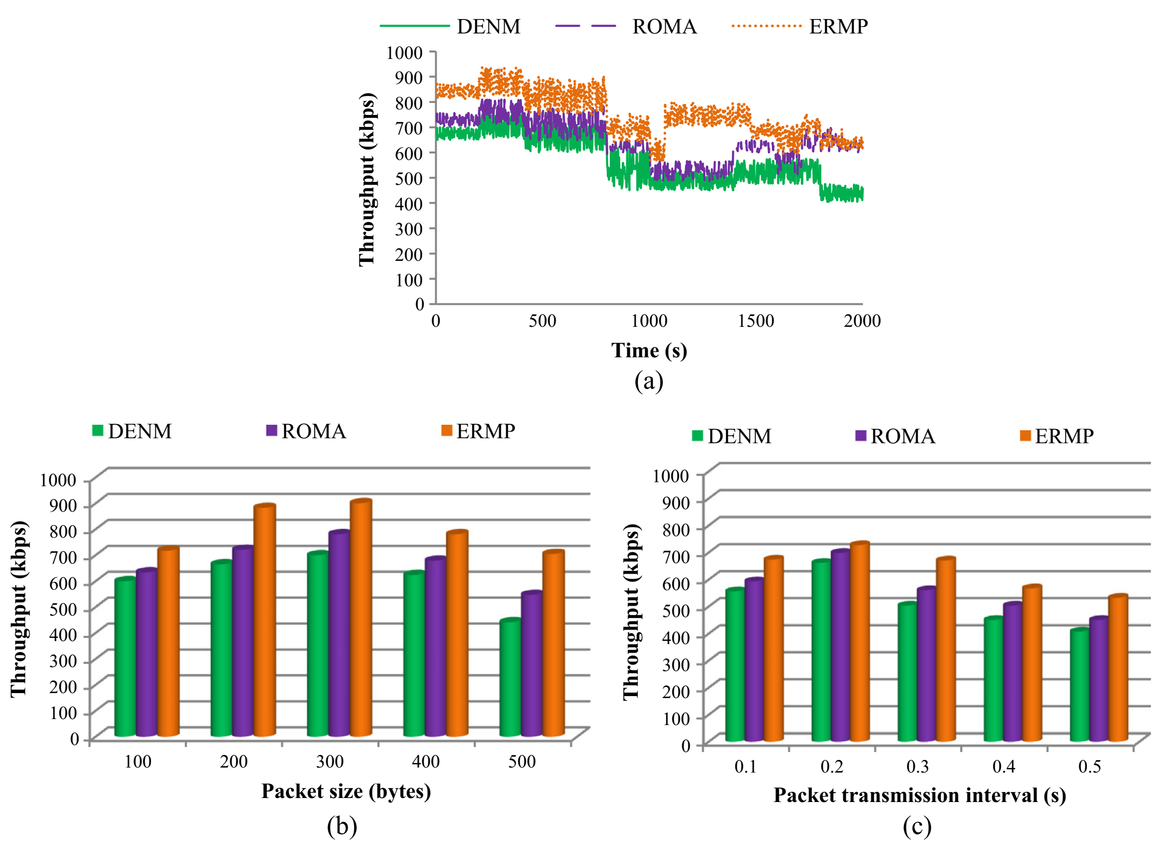

Figure 9 (a) Throughput vs. time. (b) Throughput vs. packet size. (c) Throughput vs. packet transmission interval.

devices were selected. The numbers of nodes and links are considered as a realistic use of Bluetooth in our daily life for typical applications Emre and Oznur, 2006). The RWMM was used as a mobility model. The Round Robin (RR) algorithm was used for scheduling. A CBR traffic model was taken to generate the data traffic for each routing link. The whole simulation run time was set to 1000 s. The simulation was run ten times and the results were obtained by averaging those ten-time simulations. Each parameter was evaluated against the simulation time, packet size and packet interval. Packet interval is a small pause between packet transmissions; it is analyzed that the packet interval seriously affects simulation results. A long packet interval may reduce throughput and slot utilization. On the other hand, a short packet interval may increase healing delay and increase control packet overhead. Therefore, the packet interval should be wisely selected. After getting the comparison results, it was analyzed that the proposed ERMP protocol outperformed the existing protocols.

The successfully repaired links demonstrated how many failed links had been repaired. The proposed ERMP was compared with the previous DENM and ROMA protocols and it is observed from Fig. 8, that the proposed ERMP successfully repaired more links as compared to the ROMA and DENM protocols. The proposed ERMP predicted the weak links when the distance increased between the connected routing devices. Thus to overcome the link disconnection problem, the ERMP dynamically activated a new link before the main link disconnected. An example, shown in Fig. 3(b), shows how the ERMP repaired the weak routing links before the main route breakage. Once the main route broke, the devices started to search for a new route through inquiry and the inquiry procedure; thus, unnecessary resources were consumed by the system. ROMA did not provide a solution for the route recovery on run time when an active routing link disconnected. It started a new link process from the inquiry scan which consumed more time. On the other hand, the DENM protocol just predicted the energy level of the devices. When it predicted a lower energy level, it activated a backup device but it did not provide any solution when a link broke because of mobility. Therefore, DENM has repaired fewer numbers of routes compared to ERMP.

Throughput can be defined as the successful delivery of data packets per unit time across the network. It is observed from Fig. 9, that the overall throughput of the proposed ERMP was higher than the ROMA and DENM protocols. During the simulation, the same numbers of data packets were routed across the network using the ERMP, ROMA and DENM protocols. It was noted that the total numbers of received packets through the ERMP were more than the other protocols because it prevented the main routing link being broken and it always maintained the network transmission by predicting the status of the routing devices. Whereas, the throughput of the ROMA protocol was less than the proposed protocol, because once the main links broke it created all new links for the existing devices. Thus, ROMA increased the number of piconets which degraded the network performance. It was also analyzed that the throughput of the DENM protocol was also less than the ERMP. Due to the mobility; if the main link broke, it did not perform any action so it could not receive all of the data packets. Therefore, the proposed ERMP is con-

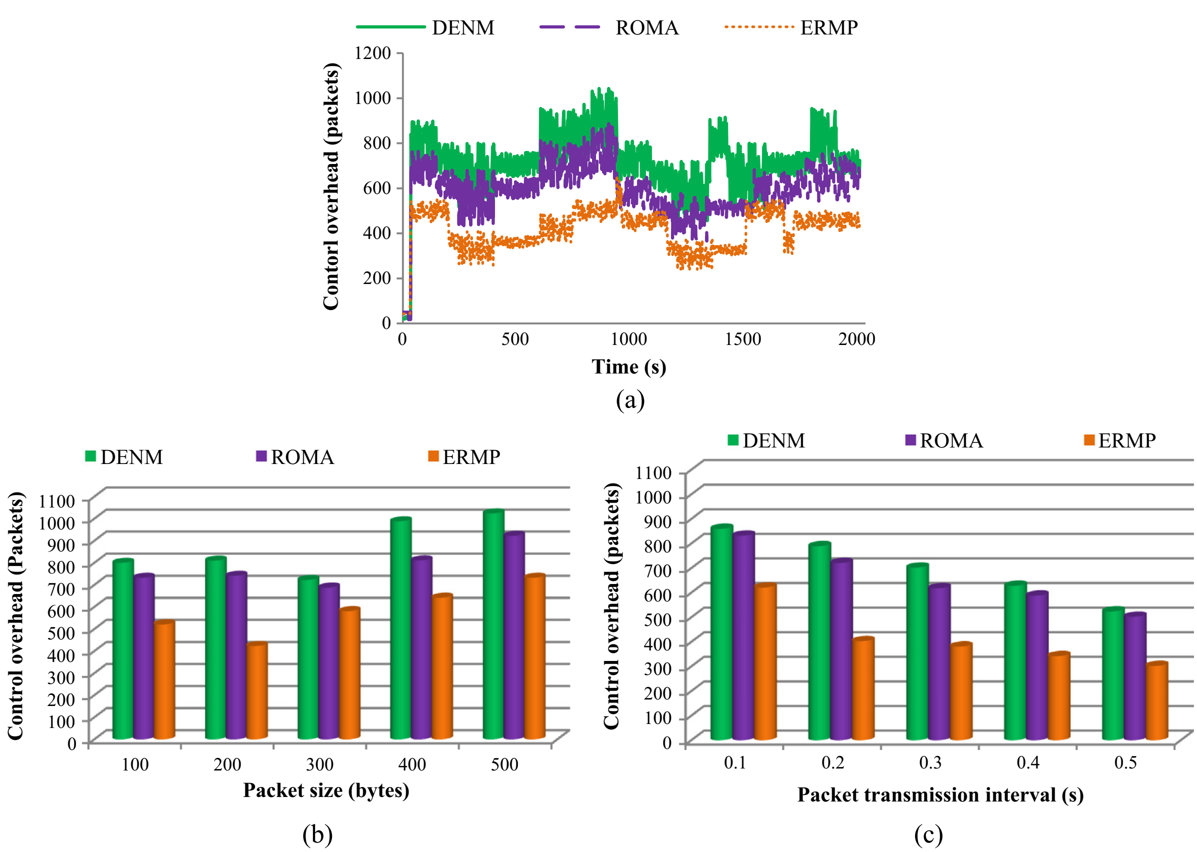

Figure 10 (a) Control overhead vs. time. (b) Control overhead vs. packet size. (c) Control overhead vs. packet transmission interval.

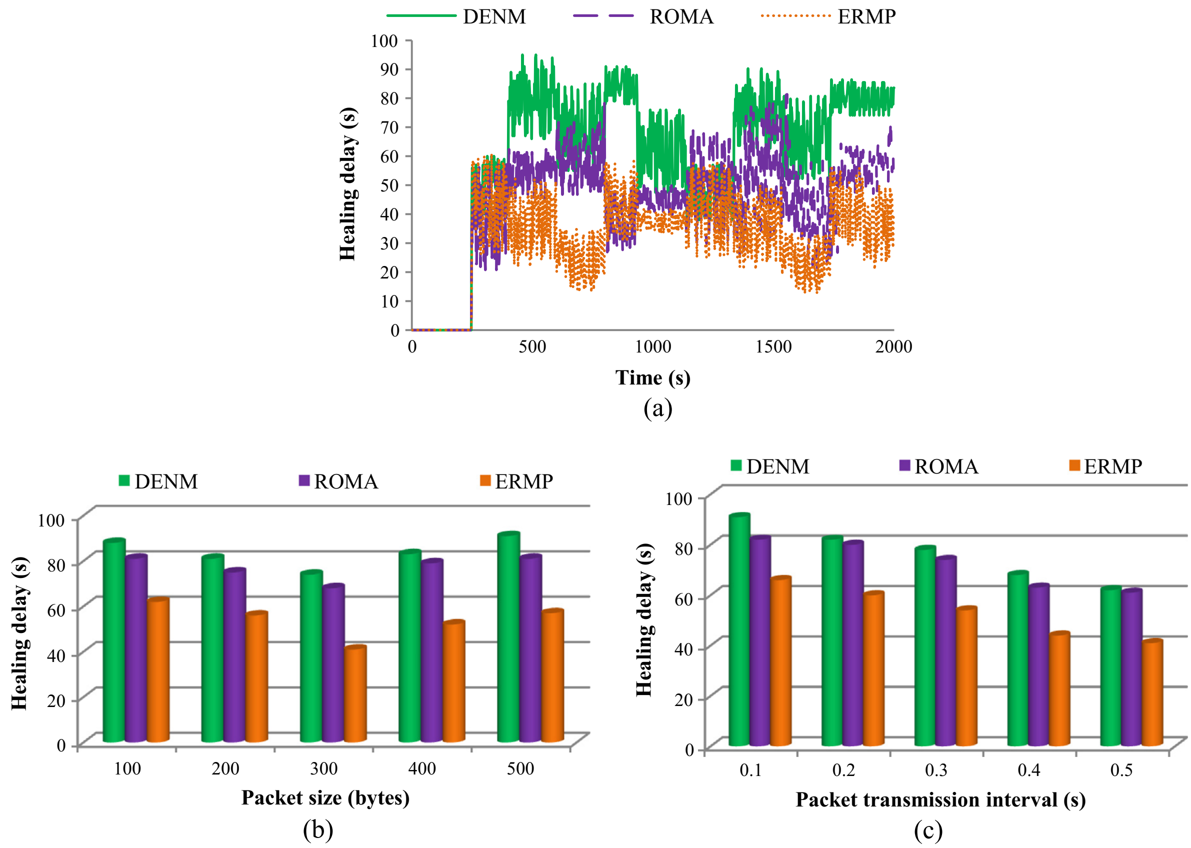

Figure 11 (a) Healing delay vs. time. (b) Healing delay vs. packet size. (c) Healing delay vs. packet transmission interval.

sidered as a more efficient protocol than the previous ROMA and DENM protocols.

Bluetooth devices use control packets for transmission, synchronization and connection. It has been analyzed that due to limited battery power and mobility, Bluetooth frequently performs network restructuring consuming extra control packets that ultimately degrades the network performance. Therefore, if the battery power and mobility of a device is predicted, it can reduce frequent link disconnection that can ultimately reduce control overhead. Control message overhead is calculated as, the sum of MAC, NULL, bb and POLL. From Fig. 10, it is observed that the proposed ERMP has less control packet overhead compared to the DENM and ROMA protocols because both protocols did not perform network restructuring for route maintenance. Whereas, the proposed protocol reserved the information of the FBDs and whenever a weak link or weak device was predicted, it activated the FBD and saved the extra resource utilization. A device was selected as a backup device if it was connected with the same piconets and could support the disconnected links. Although ROMA is a route maintenance protocol, it changes the overall network structure which creates unnecessary control overhead. It can be analyzed that the proposed ERMP control packet overhead is the least in all three protocols.

Fig. 11 shows the healing delay of the protocols. After getting the simulation results, it was observed that the proposed ERMP consumed the minimum route recovery time as compared to the ROMA and DENM protocols. The reason behind this was that the proposed ERMP is based on the prediction of weak links and weak devices and it always keeps the information of the FBDs for the route maintenance on run time. As the existing protocols start a new link procedure form inquiry and the inquiry scan procedure, which take 10.28 s. While, the proposed ERMP repairs the weak links, it starts from the paging process that takes the maximum time of 2.56 s for each link. The DENM protocol takes more time as compared to the ERMP because it predicts the devices based on the energy level; if a device having a critical energy level is predicted, it activates a backup device. When it repairs the links by activating the backup device, it starts from the paging process that takes 2.56 s for each link. In case a link fails due to the mobility, it starts to re-establish the link and performs the inquiry, inquiry scan, page and page scan processes; that takes a longer time. The DENM route recovery for each link takes (2.56 s + 10.24 s), therefore, it takes more time compared to the ERMP. On the contrary, the ROMA requires a longer healing time for route maintenance because it maintains the routing link if any device joins or leaves the network, however, it does not perform any action if suddenly a link breaks or device fails. ROMA reconstructs the routing paths if the communication between the networks stops; it also starts from the inquiry processes. Therefore, the ROMA also increases healing delay compared to ERMP.

New connections were blocked when the numbers of requests increased or active links were disturbed. From Fig. 12, it is observed that the ROMA and DENM protocols blocked more connections. As DENM only considers the low energy level of a device, it did not provide the solution if any routing device moved away and broke the link. When devices were disconnected due to mobility between the main

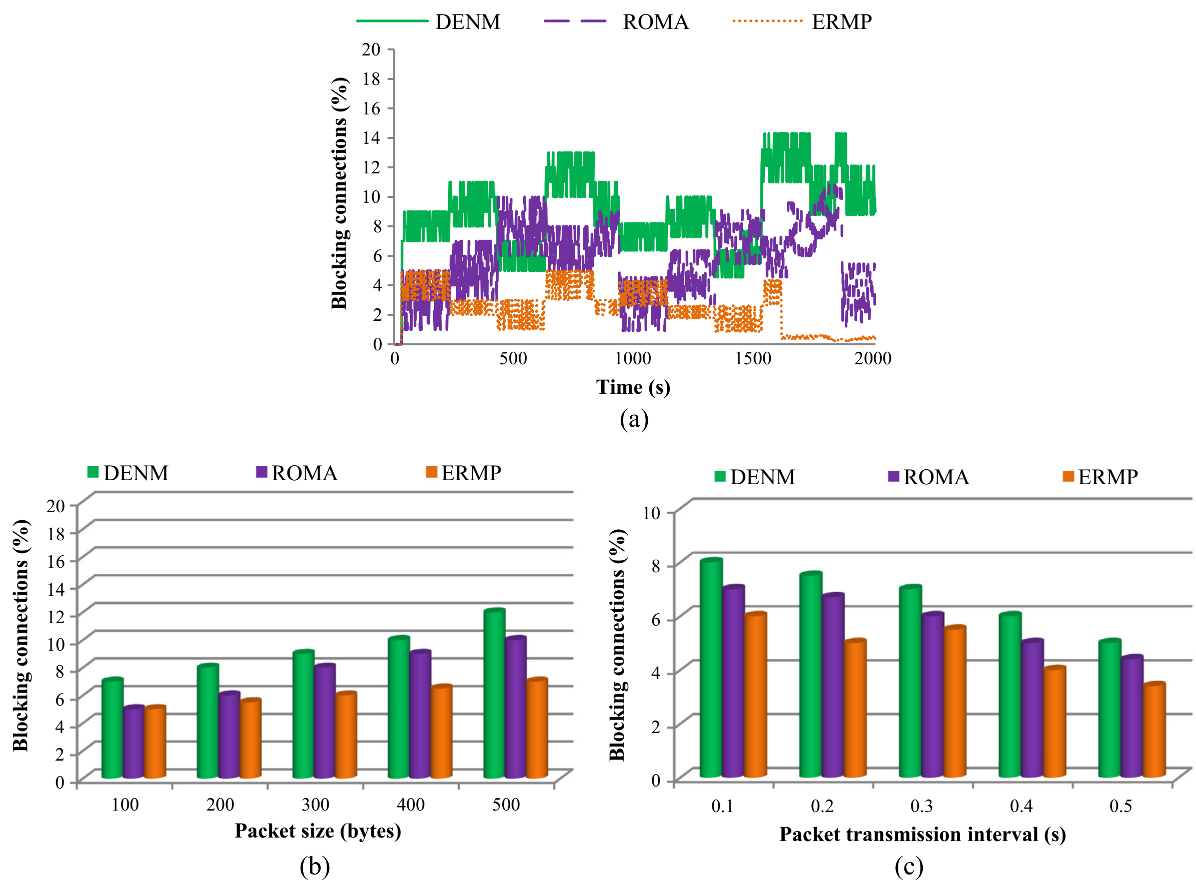

Figure 12 (a) Blocking connections vs. time. (b) Blocking connections vs. packet size. (c) Blocking connections vs. packet transmission interval.

routing links, the DENM blocked more connections. On the contrary, ROMA did not provide the best solution for broken links. Mostly, source and intermediate devices were unable to forward the data to the destination device due to a link failure. It has been analyzed that the proposed ERMP reduced the blocking percentage compared to the previous DENM and ROMA protocols. It has also been observed that as the number of devices increased it also increased the network size, which increased the path length. For the longer path, more numbers of intermediate devices were used, which increased the chances of link breakage.

It is analyzed from Fig. 13 that the overall slot utilization of the proposed ERMP was higher than the ROMA and DENM protocols. During the simulation, the same numbers of data packets were routed across the network using the ERMP, ROMA and DENM protocols. It was noted that the total number of received packets through the ERMP was more than the other protocols because it prevented the main routing link from being broken and it always maintained the network transmission by predicting the status of the routing devices. Whereas, the slot utilization of the ROMA protocol was less than the proposed protocol, because once the main links broke, it created all new links for the existing devices. Thus, ROMA increased the number of piconets which degraded the network performance. It was also analyzed that the slot utilization of the DENM protocol was also less than the ERMP. Due to the mobility, if the main link broke, it did not perform any action so it could not utilize available slots. The proposed ERMP is considered as more efficient in terms of slot utilization due to route maintenance functionality compared to ROMA and DENM.

5. Conclusion

In this paper, an Efficient Route Maintenance (ERMP) Protocol is proposed for dynamic Bluetooth networks. During the main route construction each routing master and routing bridge device keeps the required information of all the connected devices. The proposed protocol predicts the weak links and weak devices through the signal strength and energy level of the devices and repairs the weak routing path by activating the FBDs. Our analysis showed that ERMP is more efficient compared to ROMA and DENM because both the protocols provide a solution for route breakage only when the main route is broken. On the contrary, the proposed protocol predicts the weak routing links and the weak devices, if a weak routing link is notified the proposed protocol introduces a new link before the main route is damaged. The simulation results reveal that the ERMP outperforms the existing protocols in terms of repairing connections, healing delay, control overhead, blocking connections and slot utilization.

Every research work has a future direction, which provides the opportunity for future research continuation in the field. The proposed ERMP can be extended in future to select a

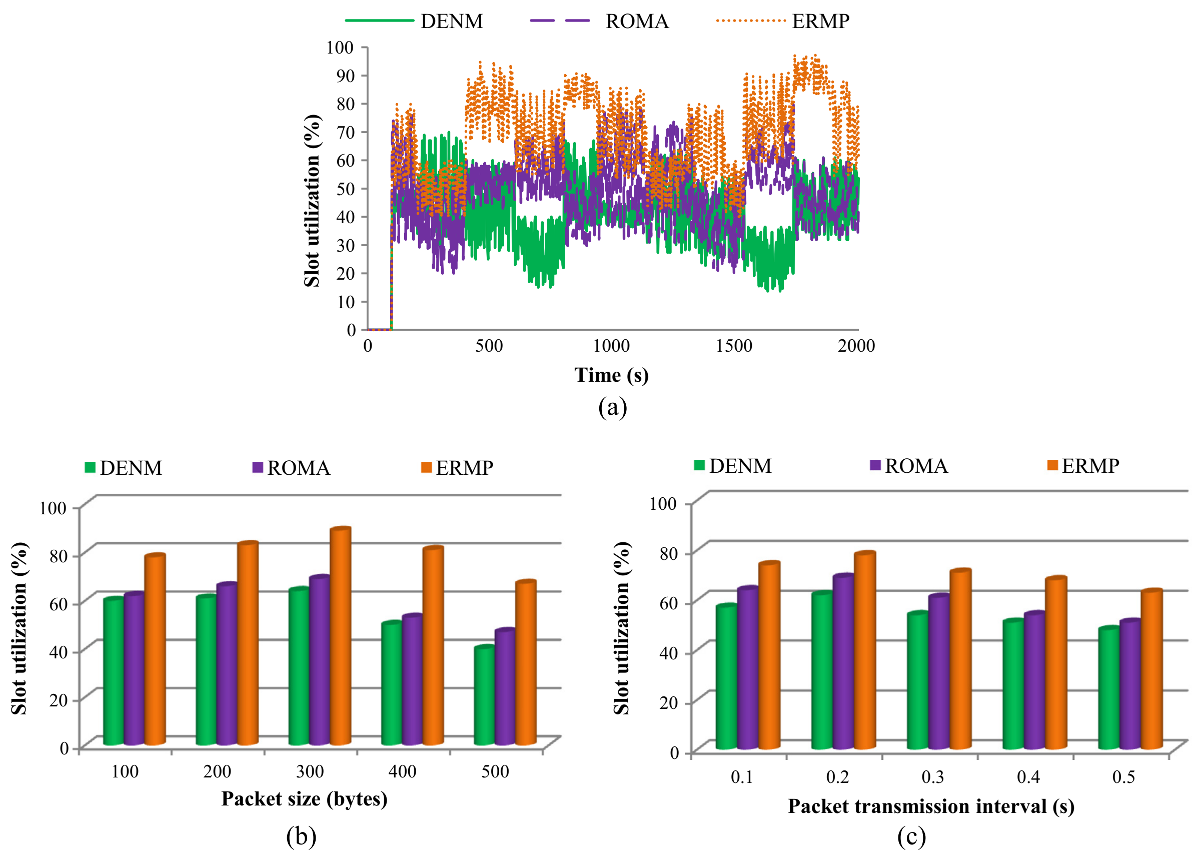

Figure 13 (a) Slot utilization vs. time. (b) Slot utilization vs. packet size. (c) Slot utilization vs. packet transmission interval.

relay based on relay mobility. The plan is to enhance the ERMP in such a way that a backup device can be adjusted in a piconet where it is frequently communicating. This is necessary to support the problem of link disconnection due to user mobility.

References

Agrawal, D., Wang, Q., 2007. University of Cinicinnati Bluetooth Simulator (UCBT), Online: <http://www.cs.uc.edu/~cdmc/ucbt/>.

Aldabbagh, G. et al, 2015a. QoS-Aware Tethering in a heterogeneous wireless network using LTE and TV white spaces. Comput. Netw. 81, 136–146.

Aldabbagh, G. et al, 2015b. Distributed dynamic load balancing in a heterogeneous network using LTE and TV white spaces. Wirel. Netw., 1–12

Bakhsh, S.T. et al, 2011. Dynamic energy-aware network maintenance for Bluetooth. In: International Conference of Information Science and Applications.

Bo, H. et al, 2012. Mobile data offloading through opportunistic communications and social participation. IEEE Trans. Mob. Comput. 11 (5), 821–834.

Chih-Min, Y., Yin-Bin, Y., 2014. Reconfigurable algorithm for bluetooth sensor networks. Sens. J. IEEE 14 (10), 3506–3507.

Ching-Fang, H., Shu-Ming, H., 2008. An adaptive interpiconet scheduling algorithm based on HOLD mode in bluetooth scatternets. IEEE Trans. Veh. Technol. 57 (1), 475–489.

Cui, Y.-D. et al, 2010. Bluetooth energy-saving optimization: a queuing theory analysis. J. Chin. Univ. Posts Telecommun. 17 (Suppl. 1), 54–57.

Emre, A., Oznur, O., 2006. A classification and performance comparison of mobility models for Ad Hoc networks. In: ADHOC-NOW. Springer, Istanbul, Turkey, pp. 444–457.

Etxaniz, J., Aranguren, G., 2015. Modeling of the data transportation network of a multi-hop data-content-sharing home network. IEEE Trans. Consum. Electron. 61 (1), 31–38.

Jin-Ho, C., Guang, G., Kyeongcheol, Y., 2014. New families of optimal frequency-hopping sequences of composite lengths. IEEE Trans. Inf. Theory 60 (6), 3688–3697.

Kuo Hsing Chiang, 2004. A 2D Random Walk Mobility Model for Location Management Studies in Wireless Networks.

Laharotte, P.A. et al, 2015. Spatiotemporal analysis of bluetooth data: application to a large urban network. IEEE Trans. Intell. Transp. Syst. 16 (3), 1439–1448.

Ramana Reddy, G. et al, 2010. An efficient algorithm for scheduling in bluetooth piconets and scatternets. Wirel. Netw. 16 (7), 1799–1816.

Sahoo, P.K., Chang, C.-Y., Chang, S.-W., 2008. Novel route maintenance protocols for the Bluetooth ad hoc network with mobility. J. Netw. Comput. Appl. 31 (4), 535–558.

Sharafeddine, S., Al-Kassem, I., Dawy, Z., 2012. A scatternet formation algorithm for bluetooth networks with a non-uniform distribution of devices. J. Netw. Comput. Appl. 35 (2), 644–656.

Singh, P., Agrawal, S., 2011. A servey on bluetooth scatternet formation. In: Wyld, D. et al. (Eds.), Advances in Computing and Information Technology. Springer, Berlin Heidelberg, pp. 260–269.

Subhan, F. et al, 2011. Handover in bluetooth networks using signal parameters. Inf. Technol. J., 965–973

Subhan, F. et al, 2012. Analysis of bluetooth signal parameters for indoor positioning systems. In: International Conference on Computer & Information Science (ICCIS), pp. 784–789.

Tahir, S. et al, 2013. Hybrid congestion sharing and route repairing protocol for bluetooth networks. In: International Conference on Electronics, Signal Processing and Communication Systems, pp. 33–39.

The Network Simulator (NS-2), 2014. Online: <http://www.isi.edu/nsnam/ns/ns-build.html>.

Xin, Y., YuPing, W., 2009. Secure constructing bluetooth scatternet based on BTCP. In: Information Assurance and Security, 2009. IAS '09. Fifth International Conference on.

Yu, C.-M., 2010. A study on the topology control method for bluetooth scatternet formation. In: Pan, J.-S., Chen, S.-M., Nguyen, N. (Eds.), Computational Collective Intelligence. Technologies and Applications. Springer, Berlin Heidelberg, pp. 263–271.

Yu, C.M., 2012. Global configured method for blueweb routing protocol. IET Commun. 6 (1), 69–75.

Yu, C.M., Lin, J.H., 2012. Enhanced bluetree: a mesh topology approach forming bluetooth scatternet. IET Wirel. Sens. Syst. 2 (4), 409–415.