ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

Efficient Key Distribution and Key Computation Using EBR in Bluetooth SSP

R.Manimala [1], M.Jeyasudha [2], M.Nelgadevi [3]

Assistant Professor, Department of IT, Sri Paramakalyani College, Alwarkurichi, Tamilnadu,India[1]

Assistant Professor, Department of IT, Sri Paramakalyani College, Alwarkurichi, Tamilnadu,,India[2]

Assistant Professor, Department of CS, Rani Anna Government College for women, Tirunelveli, Tamilnadu,India[3]

Abstract: Bluetooth is a wireless technology which enables communication between Bluetooth-compatible devices such as mobile phones, computers, PDAs etc. Security is the major concern during wireless communication. There are possibilities of two Man In The Middle attack (MITM) on Bluetooth Secure Simple Pairing(SSP) .First Attack is based on the falsification of information sent during the input/output capabilities exchange named as Bluetooth - No Input, No Output - Man-In-The-Middle (BT-Nino-MITM) attack. Second attack is Bluetooth - Secure Simple Pairing - Out-Of-Band - Man-In-The-Middle (BT-SSP-OOB-MITM) attack requires some kind of visual contact to the victim devices in order to mislead the user to select a less secured Just Work (JW) association model instead of using a more secure Out Of Band (OOB) channel [1]. In this paper, we proposed key distribution and key computation scheme, where the cluster head (master node) establish unique key for each node in a cluster and computes a session key in each session for secure communications over an unreliable wireless network. The session key provides group secrecy and source authentication since it reduce the possibilities of Man In he Middle Attack (MITM). Secret sharing and power efficiency is important in order to ensure secure communication. Since, we proposed Energy Based Routing algorithm for low power consumption during secret sharing. In addition, we provided comparative analysis with Dynamic Source Routing and Destination Sequenced Distance-Vector Routing algorithms.

Keywords: Man In the Middle Attack, Simple Secure Pairing, Energy Based Routing, key distribution, Key Computation.

I. INTRODUCTION

Bluetooth is an ad hoc networking technology which dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station. Two Bluetooth nodes are considered to be in sync when they share the same clock value and frequency-hopping pattern. A Bluetooth can have one master device and seven active slave devices as well as unlimited passive (parked) slaves. A master and its associated slaves form a piconet. A scatternet is formed by two or more piconets that share common Bluetooth nodes. Scatternet allows several devices to be networked over an extended distance in a dynamic topology that can change during any given session.

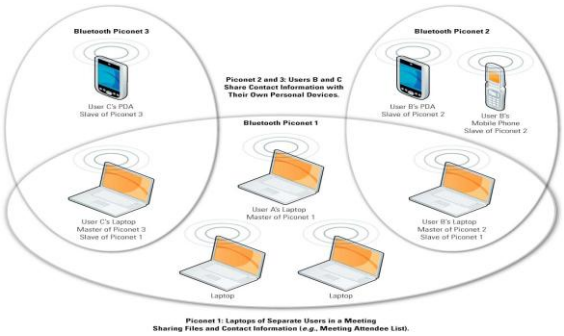

FIG. 1 Scatternet (Bluetooth Ad hoc network)

Bluetooth pairing occurs when two Bluetooth devices agree to communicate with each other and establish a connection. In order to pair two Bluetooth wireless devices, a password (passkey) has to be exchanged between the two devices. A Passkey is a code shared by both Bluetooth devices, which proves that both users have agreed to pair with each other. After pairing the devices, a passkey is stored and authentication occurs automatically during future connections. The passcode is usually needed only once during the initial setup of the wireless device. The "pairing process" is one of the most basic levels of security for Bluetooth devices.

A. *Bluetooth Security Issues*

Bluetooth security becomes a major concern when exposing important data stored on your laptop to other devices on the Bluetooth network. Both Sony Ericsson and Nokia have admitted that the pairing process can allow an attacker to copy a phone's contacts book, calendar and other data without requiring the victim to 'pair' with another Bluetooth device. Bluetooth technology and associated devices are susceptible to general wireless networking threats such as Eavesdropping attack on the Passkey Entry Mode, Cipher attack, Location attack in which attacker is able to determine the geographic location of the victim device. Relay attacks on Bluetooth authentication protocol made for impersonation, Man-In-The Middle (MITM) attack, Denial Of Service Attacks etc. These vulnerabilities may lead to the compromise of the device and those networks to which it connects.

[1] Defines two new Man-In-The-Middle (MITM) attacks on Bluetooth Secure Simple Pairing (SSP).The attacks are Bluetooth - No Input, No Output - Man-In-The-Middle

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

(BT-Nino-MITM) attack and Bluetooth - Secure Simple Pairing - Out-Of-Band - Man-In-The-Middle (BT-SSP-OOB-MITM) attack. It propose to improve the security of SSP by adding an additional window at user interface level as well as using OOB channel as a mandatory association model to all Bluetooth device manufacturers.

[2] Analyses Man-in-the-Middle attack on Bluetooth Secure Simple Pairing. Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol enables two users to create a shared secret agreement during SSP. Both master and slave device compute the DH Key using private key of own and public key of other device as function arguments. This paper proposes modified SSP, where the two parties can use common secret cryptographic function to compute a symmetric key that will be used to encrypt the commitment value.

[3] defines self-healing key distribution scheme which allow group managers to broadcast session keys to large and dynamic groups of users over unreliable channels. This paper proposes a new definition of self-healing key distribution, and show that it can be achieved by concrete schemes.

[11]Self-healing key distribution schemes are particularly useful when there is no network infrastructure or such infrastructure has been destroyed. A self-healing mechanism can allow group users to recover lost session keys and is therefore quite suitable for establishing group keys over an unreliable network. This self-healing key distribution scheme can sponsor a new user to join the group for the subsequent sessions without any interaction with the group manager.

[8]Ad hoc networks have brought many varieties of applications for mobile digital devices but batteries carried by each mobile node have limited power. This paper proposes a novel adaptive cluster-head algorithm for ad hoc networks based on Bluetooth technology, which selects candidates for cluster-head by fuzzy logic algorithm and generates a flexible structure to share the power consumption and traffic load with the cluster-head dynamically.

B. Man-In-The-Middle attack

Man-In-The-Middle attack is the type of attack where attackers intrude into a connection to intercept the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying the data.

C. Power Consumption in Bluetooth

Energy resource is one of the most important resources in ad hoc networks where terminals are always supplied with limited battery. The way the devices are grouped in different piconets and the way the piconets are interconnected greatly affect the performance of the scatternet in terms of capacity, data transfer delay, and energy consumption.

There are quite a number of routing protocols that are excellent in terms of efficiency. Thus, when considering extending the lifetime of the mobile devices, as well as the lifetime of the whole network, energy efficiency of routing protocols is a prominent issue.

II. PROPOSED WORK

A. Establishing wireless links between dynamic nodes

Bluetooth allows users to form ad hoc networks between a wide variety of devices to transfer voice and data. It provides a mechanism for creating small wireless networks on an ad hoc basis, known as piconets as shown in Fig. 2. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence. An example of a piconet is a Bluetooth-based connection between a cellular phone and a Bluetooth-enabled laptop. In a piconet, one device serves as the master, while all other devices in the piconet acting as slaves. Piconets can scale to include up to seven active slave devices. The master device controls and establishes the network. The dynamics of a network can change the condition of a wireless link rapidly.

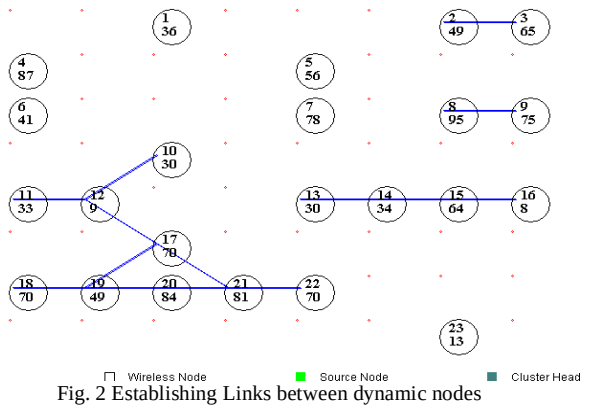

Fig. 2 Establishing Links between dynamic nodes

B. Cluster Area

Bluetooth piconets are often established on a temporary and changing basis, which offers communication flexibility and scalability between mobile devices. Nodes are arranged dynamically and find the neighbourhood node. In this work, each piconet forms a cluster as shown in Fig.3. Master node in a cluster (piconet) is considered as cluster head. Cluster heads spend more energy than leaf nodes.

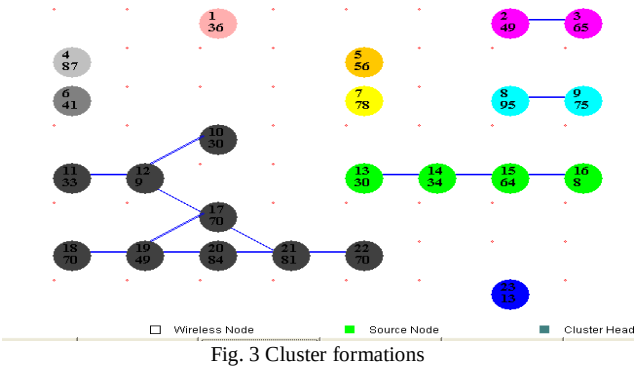

Fig. 3 Cluster formations

C. Cluster Head

A mobile ad hoc network is a dynamic wireless network that can be formed without the need for any pre-existing

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

infrastructure in which each node can act as a router. Clustering is an effective topology control approach in mobile ad hoc networks, prolonging the lifetime and improving the capability of networks. In order to maintain the stability of clusters, energy of mobile nodes and connectivity are taken as the basis of cluster head election. Selecting the node which has most weight and stability to be the cluster head. Clustering is one of the techniques used to manage data exchange amongst interacting nodes. Moreover, Cluster heads should be capable of sustaining communication with limited energy sources for longer period of time. In this context, selection of best cluster heads with trusted information becomes critical for the overall performance. It aims to elect trustworthy stable cluster head that can provide secure communication via cooperative nodes. The tasks of session key management are to provide: (i) node identification and authentication, (ii) access control and (iii) management of keying material including the session key and all the supporting keys. Election of cluster-head is based on a probability, which might be energy-aware as shown in Fig. 4. The node with most residual energy among its neighbours is elected as cluster-head in that cluster.

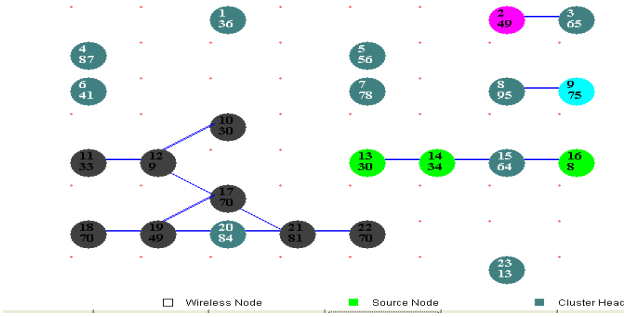

Fig. 4 Cluster Head Election

D. Key Distribution

Cluster head creates unique key randomly for each node in a cluster for each session as shown in Fig. 5.

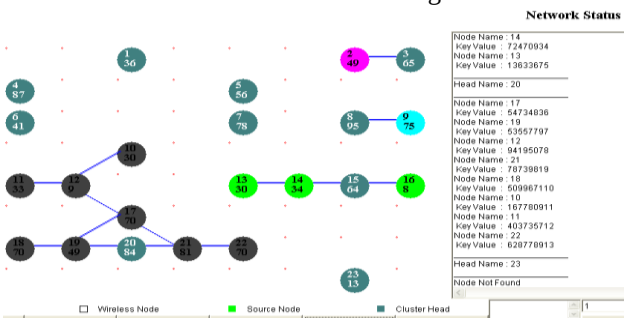

Fig. 5 Cluster Head distributing unique key for each member in the cluster

The random challenge, which is a public parameter associated with the authentication process, is designed to be different for every transaction. The random number is derived from a pseudo-random process within the Bluetooth device. Cluster head distributes unique keys to different members in the cluster. This is each cluster member's secret key and is distributed through a secure communications channel between the cluster head and the individual node. Unique key distribute by the cluster head is known only to the cluster members effectively protect a multicast group.

The cluster head randomly picks a 2t-degree masking polynomial [5], $h(x) = h_0 + h_1x + ... + h_{2t}x^{2t}$, from Fq[x]. Each node U_i gets the Unique key f (i), $S_i = \{h(i)\}$, from the cluster head via the secure communication channel between them. The cluster head constructs polynomial w(x) such that for a selected cluster node U_i, f(i) can be recovered from the knowledge of w(x) and the session key S_i, but for any revoked group member $U_{i'}$, f(i') cannot be determined from w(x) and $S_{i'}$. Since the adversary cannot get any information about keys.

E. Key Computation

Lifetime of a wireless network is partitioned into time intervals called session .cluster head computes the session key based on the unique keys for each session as shown in Fig. 6. The session keys are updated periodically, where the update is performed regardless of changes in network (cluster) topology. . Secure cluster communication relies on secure and robust creation of session key. Duration of session is dynamic, session key is updated each time when new node joins or existing node leaves the cluster. The newly joint users should not be able to derive the previous session key. Similarly, the revoked users who leaves the cluster in a particular session and again join in that cluster should not be able to derive the future session key, even if they are able to compute the previous session keys with previously distributed keying information. MITM attack caused due to the lack of security during Simple Secure Pairing .The aim of MITM attack is impersonation where the attacker acts just before the legitimate user. In this proposed scheme, MITM attacks against SSP are prevented by session key. Adversary unable to compute the session key for attacking the victim devices in a cluster during a session. Periodic rekeying can significantly reduce both the computation and communication overhead and thus improve the scalability and performance of key distribution.

Fig. 6 Cluster Head computing session key

The cluster head also picks m random session key [5], $\{S_i\}$ i=1, m $\in$ Fq and m random t-degree polynomials $p_1(x)$, ..., $p_m(x)$ from Fq[x]. It evaluates the polynomials $\{P_{j,i}(x)\}i=1,...,j$ and $\{Q_{j,i}(x)\}i=j,...,m$ at point v, recovers the shares $\{p_1(v), ..., p_j(v)\}$ and $\{q_j(v), ..., q_m(v)\}$, and computes the current session key by $S_j = p_j(v) + q_j(v)$.

F. Secret Sharing

In a cluster , unique key is an secret key for each cluster members and is distributed through a secure communications channel between the cluster head and the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

individual nodes .The devices share the information from source to destination secretly using the session key computed based on the unique keys of cluster members. The main concept of key distribution schemes is that the users in a dynamic group communicate over an unreliable network, transfer information only for trusted members in that cluster as shown in Fig.7.

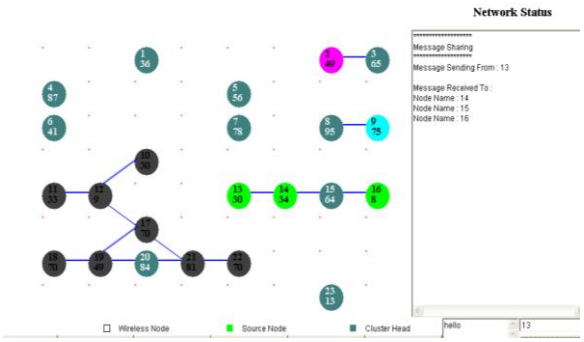

Fig.7 Secret sharing between trusted members in the cluster

G. Revoke

If a node disconnected from the network, cluster head make that node as inactive as shown in Fig.8. This paper provides computationally secure and efficient key distribution scheme with self-healing property for node revocation in the dynamic groups. Revoked node can reinstate in its cluster using the unique key. Cluster head construct new session key during the time it was revoked. Periodic rekeying prevents the unauthorized person to enter the cluster. The cluster head picks m random session key [5], $\{S_i\}$ i=1, m ϵ Fq and m random t-degree polynomials $p_1(x)$, $p_m(x)$ from Fq[x]. For each $p_i(x)$, the cluster head constructs $q_i(x) = S_i - p_i(x)$.

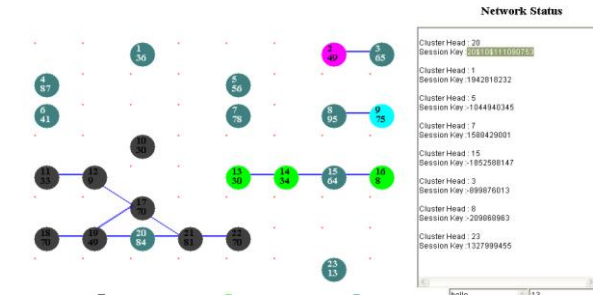

Fig.8 Cluster head change the session key when node (10) leaves the cluster.

H. Self Healing

Self-healing means the network adapts automatically to defects and attacks in its node connectivity, service provisioning and performance disturbances to provide the security to the communicating parties. In this scheme, self healing technique is used, to make a node as acceptable in same cluster after sleeping, using previous unique key as shown in Fig.9. The self-healing capability enables a routing based network to operate when one node breaks down or a connection goes bad. In the jth session key distribution[5], give the unique key of revoked node for sessions in and before session j, $R_i = \{r_1, r_2, ..., r_{wi}\}i=1,...,j$, where $|R_i| = w_i \leq t$ for i = 1, ..., j. When a non-revoked cluster node U_v receives the jth session key distribution message, it evaluates the polynomials $\{P_i(x)\}i=1,...,j$ and $\{Q_i(x)\}i=j,...,m$ at point v,recovers the shares {p1(v), ..., p_j (v)} and {q_j(v), ..., q_m(v)}, and computes the current session key $S_j = p_j(v) + q_i(v)$.

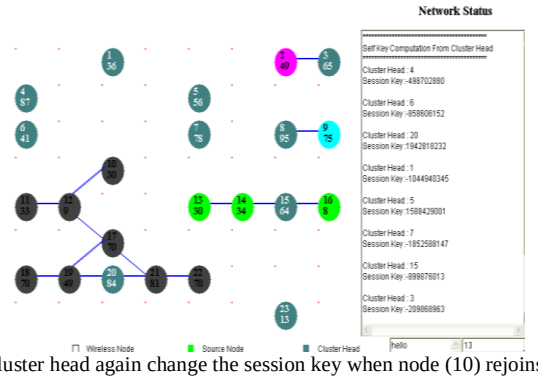

Fig.9 Cluster head again change the session key when node (10) rejoins its cluster with the unique key

I. Sponsorization

If a new node enter the cluster during a session , n/2 nodes of that cluster should sponsor for the newly entered node as shown in Fig.10. The keys are securely redistributed to the members of the cluster .Based on the rekeying, the session keys are updated periodically, when new users join the cluster. Only legitimate users should have access to the cluster communication in order to achieve privacy. The newly joined users should not be able to derive the previous session keys, even if they are able to derive future session keys with subsequently distributed keying information. Similarly, the revoked users should not be able to derive the future session keys, even if they are able to compute the previous session keys with previously distributed keying information.

When the cluster head wants to add a new node starting from session j with n/2 nodes sponsorization, [5]It picks an ID v ϵ F_q, which is never used before, computes all $\{h_i,_k(v)\}i=j,...,m, k = j,...,m+1$, and gives {v, $\{h_i,k(v)\}I$ = j,...,m,k=j,...,m+1} to the cluster nodes via the secure communication channel between them. It computes $(l,f(l,f_id_j))$ from his Unique key f(l,y) and sends it to privately to U_i.cluster head computes $s(i,s_id_j)$,$P_j(i)$ and $r_j(i)$ after receiving n/2 sponsored messages from the nodes. Therefore, he can compute s (i, sidj). Consequently, cluster head compute the session key as: $K_j = P_j(i) - s(i, s_id_j) / r_j(i)$.

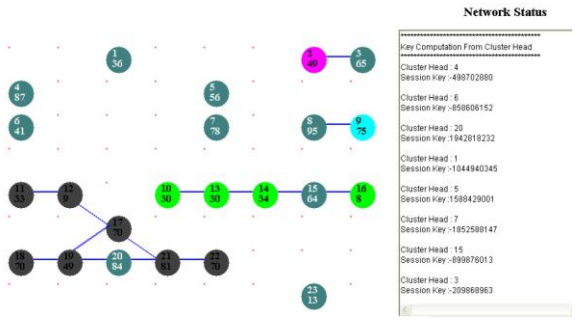

Fig.10 Node (10) joins in another cluster (15) with the sponsorization capability

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

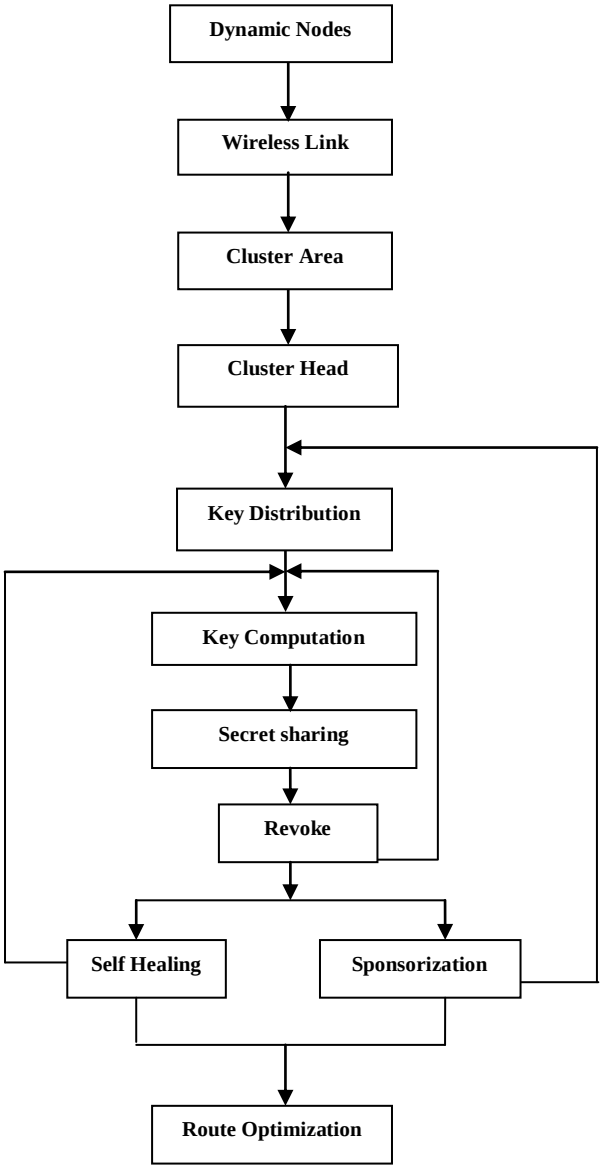

Fig.11 Architecture of the proposed system.

J. Route optimization

Self-healing is a good property for key distribution in wireless mobile and ad hoc networks, where the nodes/devices are powered by batteries and have the unique feature of moving in and out of range frequently. Reducing the computation and active communication can significantly reduce the power consumption and prolong the lifetime of wireless devices. Secret sharing is done by path optimization.

The paper compares the performance of proposed Energy Based Routing algorithm with two existing algorithms such Dynamic Source Routing and Destination Sequenced Distance-Vector Routing.

1) Dynamic Source Routing (DSR) Algorithm

DSR is a reactive protocol which allows mobile sources to discover paths towards any desired destination dynamically. The reactive routing protocols are based on some sort of query-reply dialog which proceed for establishing route(s) to the destination only when the need arises. [9]The route cache is used in DSR protocol to store all the routes are learned from the source node to avoid unnecessary route discovery process. Dynamic source routing (DSR) protocol utilizes source based routing rather than table-based, and source initiated rather than hop-by-hop.

DSR protocol consists of two main functions such as route discovery and route maintenance. In this protocol, the mobile nodes are required to maintain route caches or the known routes. The route cache is updated when any new route is known for a particular entry in the route cache .If there is a data packet to transfer, the route check state checks the availability of the route in the cache memory. If already there is an entry for that destination, the source uses that to send the packet else route discovery process is initiated by broadcasting Route Request packets to the router nodes until it reaches the destination node. This request includes the destination address, source address, and a unique identification number. Each intermediate node checks whether it knows about the destination or not. If the intermediate node does not know about the destination, it again forwards the packet and eventually this reaches the destination. A node processes the route request packet only if it has not previously processed the packet and its address is not present in the route record of the packet. A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination.

TABLE I CLASSIFICATION OF RESULTS OBTAINED BY DSR ALGORITHM

ROUTES	ENERGY REQUIRED	ROUTE EVALUATION TIME	PACKET EVALUATION TIME
3	0.00434	3.0ms	6.5ms
2	0.00167	1.5ms	2.5ms
5	0.00400	2.8ms	6.0ms
8	0.00701	5.0ms	10.5ms

The Route Request packet is stored in a table to avoid repeated route discovery. If the route discovery time exceeds, then the node goes into the idle state. The Route Reply state writes a Route Reply in a piggy back manner.

Route evaluation time, Packet evaluation time, Energy required for data transmission is evaluated using number of routes find out by DSR.

Route creation is a limiting factor of Dynamic Source Routing. In high traffic network, stale routes will be generated in the route cache which increase packet loss, long delay and reduce the efficiency.

2) Destination Sequenced Distance Vector (DSDV) algorithm

DSDV is a proactive routing protocol, which maintains routes to each and every node in the network. DSDV routing algorithm maintains a sequence number concept for updating the latest information for a route. The routing processor of protocol architecture performs the following:

1. Store and update the routing table by flooding.
2. Forwards the data packet to destination using router node.
3. Reconfigure the routing architecture.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

Proactive protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. If the network topology changes too frequently, the cost of maintaining the network might be very high. If the network activity is low, the information about actual topology might even not be. In this routing protocol, each mobile node in the network keeps a routing table. Each of the routing table contains the list of all available destinations and the number of hops to each. Each table entry is tagged with a sequence number, which is originated by the destination node. Periodic transmissions of updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. So, the routing information updates might either be periodic or event driven. DSDV protocol requires each mobile node in the network to advertise its own routing table to its current neighbours. The advertisement is done either by broadcasting or by multicasting. By the advertisements, the neighbouring nodes can know about any change that has occurred in the network due to the movements of nodes. The routing updates could be sent in two ways: one is called a ‘‘full dump’’ and another is ‘‘incremental.’’ In case of full dump, the entire routing table is sent to the neighbours, where as in case of incremental update, only the entries that require changes are sent.

TABLE II CLASSIFICATION OF RESULTS OBTAINED BY DSDV ALGORITHM

ROUTES	ENERGY REQUIRED	ROUTE EVALUATION TIME	PACKET EVALUATION TIME
18	0.02404	15.0ms	36.0ms
11	0.01102	12.0ms	16.5ms
13	0.01235	13.6ms	18.5ms
9	0.00834	7.0ms	12.5ms

Route evaluation time, Packet evaluation time, Energy required for data transmission is evaluated using number of routes find out by DSDV.
Overhead in DSDV is more when the network is large and it becomes hard to maintain the routing tables at every node. DSDV cannot handle mobility at high speeds due to lack of alternative routes. DSDV is most suitable for small networks where topology changes are limited.

3) Energy Based Routing (EBR) algorithm

EBR chooses the node with the largest amount of energy for data transmission. The nodes with more energy take heavier loads, extending lifetime of the adhoc network. Since Energy Based Routing algorithm is designed to achieve an energy balance of wireless network.EC is transmission energy cost relative to available energy, its value is low when required energy for transmission is low and available energy is high.
The algorithm chooses the node with the largest amount of residual energy to assume the burden of acting as cluster head. Therefore nodes with more energy take heavier loads, extending network lifetime.
The proposed routing algorithm uses a path with energy sufficiency as well as energy efficiency to pursue energy balance for the ad hoc network. This method ensures that the node with most residual energy among its neighbours is selected as cluster-head in that region. Being a cluster-head consumes a smaller amount of energy, just relaying internally generated data to some near-by node. [7] Sending k bits to a given distance d the energy consumption is defined by

$$E_{tx}(k,d) = \begin{cases} k_{Eelec} + k_{emp}\, d^4 ; d \geq dt \\ k_{Eelec} + k_{efs}\, d^2 ; d < dt \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where, Eelec represents the energy consumption of the radio circuitry, while efs and emp is the energy used to power the broadcast amplifier. Thus to receive k bits we need

$$E_{rx}(k) = k_{Eelec} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

This algorithm is used to create the route in which the data will be transmitted from some source c_j, through a number of intermediate nodes (c_k _ _ _ c_{k+m}) which will finally relay the data to the destination. All cluster members, will send their data to the destination by evaluating the intermediate nodes with high energy level.

TABLE III CLASSIFICATION OF RESULTS OBTAINED BY EBR ALGORITHM

ROUTES	ENERGY REQUIRED	ROUTE EVALUATION TIME	PACKET EVALUATION TIME
1	0.00100	0.5ms	1.5ms
1	6.68E-04	0.4ms	1.0ms
1	3.34E-04	0.7ms	0.5ms
1	6.68E-04	0.3ms	1.0ms

Route evaluation time, Packet evaluation time, Energy required for data transmission is evaluated using number of routes find out by EBR.
This characteristic makes the proposed algorithm different from that proposed by DSR and DSDV algorithm, which consider the best path from the next node. Here it evaluates only one path which is the best one. Through this local decision making process, a Bluetooth network can achieve energy balance and prolong the lifetime of the sensor network.
Routing capabilities supported by Bluetooth networks control the changing network topologies of piconets and scatternets and assist in controlling the flow of data between networked devices. This method does not consume all the resources of a data path, thereby allowing Bluetooth devices to maintain data flow throughout a scatternet. The paper proposes Energy Based Routing Algorithm, which chooses the node with the largest amount of energy to transfer data as shown in Fig. 12. The nodes with more energy take heavier loads, extending network lifetime.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

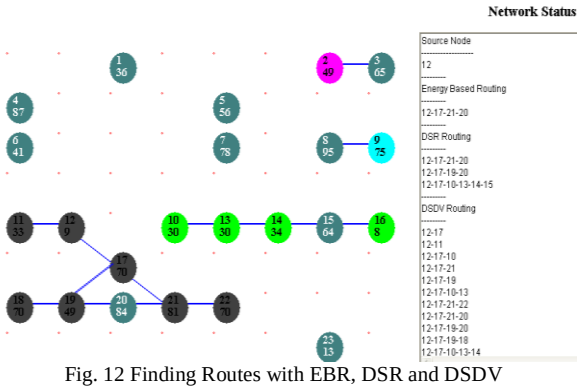

Fig. 12 Finding Routes with EBR, DSR and DSDV

III. PERFORMANCE ANALYSIS

The paper provides comparative analysis for secret sharing using efficient Energy Based Routing algorithm, which also reduces the power consumption as shown in Fig. 13. It compares the proposed routing algorithm with Dynamic Source Routing algorithm and Destination Sequenced Distance-Vector Routing algorithm.

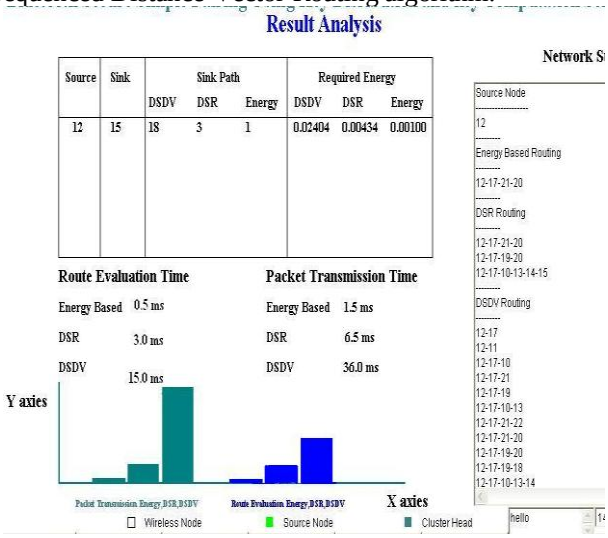

Fig. 13 Comparative analysis with EBR, DSR and DSDV

IV. CONCLUSION

This paper considered two defence strategies against MITM. First method is key distribution scheme to generate unique key for each node in the cluster .Second method is key computation to create session key for each session . Session key is updated each time ,when new node join or existing node leaves the cluster using sponsorization and self healing capability .Since Adversary unable to compute the session key for attacking the victim devices in a cluster during a session. Thus it minimizes the Man –in-the attack in the ad-hoc network during pairing. Comparative Analysis of secure routing was provided using routing algorithm. It analyse Energy Based Routing algorithm which minimize Route Evaluation time and Packet Evaluation time with two existing algorithms. Energy Based Routing produces optimal solution with low power consumption and secure routing other than DSR and DSDV routing algorithm. Bluetooth security is improved by key distribution and key computation scheme. In future it can be extended by Packet Security to avoid Bluetooth Intrusion. Wireless technology zigbee is quite similar to Bluetooth technology. This work can be extended to cover the security for these technologies.

REFERENCES

[1]Keijo Haataja and Pekka Toivanen,"Two Practical Man-In-The-Middle Attacks on Bluetooth Secure Simple Pairing and Countermeasures", IEEE Transactions on Wireless Communications, VOL. 9, No. 1, January 2010.

[2]Md. Ariful Alam and Mohammad Ibrahim Khan," Security Enhancement of Pairing and Authentication Process of Bluetooth ", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.

[3]Blundo. C.; D'Arco, P . De Santis, A.; Dipt. di Informatica ed Applicazioni, Univ. di Salerno, Fisciano, "On Self-Healing Key Distribution Schemes", Information Theory, IEEE Transactions on Volume: 52, Issue: 12, Dec. 2006.

[4]Dave Singelee and Bart Preneel, "Security Overview of Bluetooth", COSIC Internal Report, June 2004.

[5]Donggang Liu ,Peng Ning ,Kun Sun , "Efficient Self-Healing Group Key Distribution with Revocation Capability", Cyber Defense Laboratory, Department of Computer Science, North Carolina State University, Raleigh.

[6]M. Jakobsson and S. Wetzel, "Security weaknesses in Bluetooth", Lecture Notes in Computer Science, vol. 2020, pp. 176–191, Springer-Verlag, 2001.

[7]Ana Rosello,Alvin koule,Gustavo Zaninni and Brian stengaard ,"Distributed Energy Based Routing Algorithm With Deterministic Clustering", Technical university of Denmark, course 02227,Group 3, May 2008.

[8]Liu Jishun; Shen Lianfeng; Wang Xiaoxia; Zhu Xiaorong; "Adaptive Cluster-Head Algorithm for Bluetooth Ad Hoc Networks", Wireless Communications, Networking and Mobile Computing, 2007 WiCom 2007. International Conference on 21-25 Sept. 2007.

[9]Naseer Ali Husieen, Osman B Ghazali, Suhaidi Hassan, Mohammed M.Kadhum, "Route Cache Update Mechanisms in DSR Protocol – A Survey" ,International Conference on Information and Network Technology, 2011.

[10] Sanjeev Setia, Samir Koussih, Sushil Jajodia, Eric Harder, "Kronos: A Scalable Group Re-Keying Approach for Secure Multicast ",IEEE Symposium on Security & Privacy, Proc. of 2000.

[11]Song Han, Biming Tian, Mingxing He ,Elizabeth Chang ,"Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks", IEEE Transactions on Wireless Communications, April 2009.

BIOGRAPHIES

.R.Manimala Received the Master Degree in Computer Applications from SCAD college of Engineering and Technology of India in 2009 and the M.Phil. Degree in Manonmaniam Sundaranar University of India in 2012. She is working as an Assistant Professor in Sri Paramakalyani College, Tamilnadu, India. Her research interests include wireless communication and network security.

M.Jeyasudha Received the Master Degree in Computer Science from S.T. Hindu college of India in 2010 and the M.Phil. Degree in Manonmaniam Sundaranar University of India in 2012. She is working as an Assistant Professor in

Sri Paramakalyani College, Tamilnadu, India. Her research interests include Mobile computing and network security.

M.Nelgadevi Received the Master Degree in Computer Applications from SCAD college of Engineering and Technology of India in 2009 and the M.Phil. Degree in Manonmaniam Sundaranar University of India in 2010. She is working as an Assistant Professor in Rani Anna Government College for women, Tamilnadu, India. Her research interests include wireless communication and network security.