International Journal of Engineering & Technology, 7 (2.8) (2018) 661-666

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Design of data confidential and reliable bee clustering routing protocol in MANET (Vol 2)

Sajyth RB[1*], Sujatha G[2]

[1]M.Tech Information Security and cyber forensics, [2]Assistant Professor
[1,2]Department of Information technology, SRM engineering college, Kattankulathur, Chennai, India
**Corresponding Author E-mail: rbsajyth@gmail.com*

Abstract

Mobile ad hoc network (MANET) requires extraneous energy effectualness and legion intelligence for which a best clustered based approach is pertained called the "Bee-Ad Hoc-C". In MANET the mechanism of multi-hop routing is imperative but may leads to a challenging issue like lack of data privacy during communication. ECC (Elliptical Curve Cryptography) is integrated with the Bee clustering approach to provide an energy efficient and secure data delivery system. Even though it ensures data confidentiality, data reliability is still disputable such as data dropping attack, Black hole attack (Attacker router drops the data without forwarding to destination). In such cases the technique of overhearing is utilized by the neighbor routers and the packet forwarding statistics are measured based on the ratio between the received and forwarded packets. The presence of attack is detected if the packet forwarding ratio is poor in the network which paves a way to the alternate path identification for a reliable data transmission. The proposed work is an integration of SC-AODV along with ECC in Bee clustering approach with an extra added overhearing technique which n on the whole ensures data confidentiality, data reliability and energy efficiency.

Keywords: *Mobile Ad Hoc Networks, Elliptical curve Cryptography, Bee Ad Hoc Clustering, and Overhearing.*

1. Introduction

Mobile ad hoc Networks (MANETS) comprises of a group of individual nodes with mobility in an infinitesimal infrastructure less environment that communicate by forming a multi-hop radio network with each other. The nodes in MANET are capable of behaving as routers and end devices. The routing path of ad hoc networks are dynamic in character which are entirely disparate than wired networks. Thus all the security workings strategized for wired topology are annulment and not congenial for ad hoc networks.

In order to establish secure ad hoc routing protocols, the mobile nodes refashions their topology since they are pliable in character. While the transmission of data is done by the node, all the other nodes who lie in the ambient communication pasture can overhear the transmitting data by the node. If ad hoc network endure from security imminence, the routing protocols in MANET will be enormously exposed and vulnerable, precipitating numerous conjugate malicious attacks.

A MANET contains protean hubs, a switch with distinct hosts and remote esoteric gadgets. Dynamic topologies, obligated attainable transfer speed, assorted correspondence connections and confined battery are the abecedarian qualities of such systems. The nodes here are dynamic in nature which use an omnidirectional antenna and are scattered using a wireless link.

While communicating the nodes can have imperious topologies. Since MANET nodes are dynamic and self-edified in nature they are widely used from personalized requisites to defense. During data alienation necessary heed has to be taken if the transferred data stretches the destination in the determined time with lower energy devoured by the nodes. An efficient Clustered Bee Ad Hoc MANET is preferred where the transferring of data occurs in a sturdy process.

Rationale for selecting a Bee algorithm MANET is that it works similar to of swarm intelligence, here all nodes in the network are decoupled into disparate divisions based on their chores. Just as the bees in the Bee group are subdivided as Packers, Foragers and scouts, the Clustered Bee Ad Hoc MANETS are also divided as Cluster head (CH) and nodes.

In a standard Bee Clustering MANET the CH initially attempts to get the destination within the cluster by scouts or foragers, if the destination is not extant inside the cluster then help of the scout is taken where it goes out of the cluster searching the destination. But uselessly the utilization of energy by all the scouts occurs since they move arbitrarily that results in the accretion of traffic and detainment in communication. Here the energy consumption of the scout during data transfer inside the cluster by the scout is minimal when compared to that of the data transfer between one cluster to the other or to the base station. The cluster aggregates that data and sends to base station to reduce the energy consumption.

- The Infrastructure in Mobile ad hoc network is not sturdy and not credent.
- A decorous security design from source to destination should be implemented for the data confidentiality and packet delivery.
- The MANET nodes are used as routers and end devices.
- There are possibilities of data dropping attack by the nodes.

- Encryption of data packet is to be ensured before reaching the destination.
- The Cryptographic algorithms consume more power.
- An Effectual requirement of clustering algorithm in MANET is important.
- For the packet to reach from source to destination, data dropping attack should be detected and completely prevented.

2. Related Work

In Mobile Ad-Hoc Networks (MANETs), security is one of the most important concerns because a MANET's system is much more vulnerable to attacks than a wired or infrastructure-based wireless network. Designing an effective security protocol for MANET is a very challenging task. This is mainly due to the unique characteristics of MANETs, namely shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among users, limited availability of resources, and physical vulnerability. In the, simulation based study of the impact of neighbor attack and black hole attack on AOMDV routing protocol by calculating the performance metrics such as packet delivery ratio, end to end delay and throughput will be presented. The advantages are that it reduces the overhead in the network and avoids the black hole attack in the network[1]

In general, a standard sensor node can be assigned with a storage of 48kb of flash and 10kb of RAM which implies that the storage of private keys for each node is attainable but when it comes to the storage of public keys for each node is attainable but when it comes to the storage of public keys in the memory, it results to be unattainable. ECC attempts to provide a decent and a minimal sized key which provide the security at the same level as others [RSA, enTTS, NTRU] also with minimal processing time requirements and communicational overhead. ECC assigned with the 160-bit keys equalizes to the power of 1024-bit keys of RSA [2].

Since it is all the broadcast communication proceedings by nature of wireless sensor network, If the data transmitted by a node, all the other neighbor nodes who fall in the communication range in the network are liable to hear the broadcasted information. Thus, by hearing the neighbor nodes information, packet dropping attacks, reduction of delay during routing and increase the lifetime of the network can be achieved. The above hearing concept can also be stated as “overhearing” [3].

This overhearing handles the following challenges like (1) Detects if the node has too many messages in queue (prevents the dropping of packets) (2) Detects if the node instead of forwarding the collected data to the CH, forwards it to all the neighboring nodes (prevents the back-pressure messages) thus make sure to prevent unwanted bogus messages which provides network lifetime and sustainability [4].

Due to broadcasting nature in WSNs, even if the neighbor is not in direct contact, all the other neighbor nodes will be able to investigate the transmitted data, if the nodes are in broadcasted network range. This type of technique provides transparency and prevents many insider attacks [5].

Wireless Sensor Networks are characterized by having specific requirements such as limited energy availability, low memory and reduced processing power. On the other hand, these networks have enormous potential applicability, habitat monitoring, medical care, military surveillance or traffic control. Many protocols have been developed for Wireless Sensor Networks that try to overcome the constraints that characterize this type of networks.

Ant-based routing protocols can add a significant contribution to assist in the maximization of the network lifetime, but this is only possible by means of an adaptable and balanced algorithm that takes into account the Wireless Sensor Networks main restrictions. The advantages are **i**t minimizes the communication load in the network andmaximizes the energy and lifetime in the network [6]

Wireless Sensor Network (WSN) is a collaborative assertions of sensors to form a network. WSNs has a capability of monitoring the changes that can occur in physical conditions and as well as transmit the observed data via multi hop network. Since the sensors are dynamic in character, major issues were faced by the Wireless Sensor Networks (WSN) for the factors like the lifetime of sensors and the security providence by the nodes during the transmission of data are the. For generating multiple paths between source and destination, an Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol is used [7].

The main services provided by AOMDV are route discovery and route maintenance. Due to the multipath routing protocol, the lifetime of the sensors are increased since the traffic load is distributed among all the paths instead of single path in a network. Due to the dynamic character of WSNs, the malicious node introduces many attacks. One of the threat is the Warm Hole attack, a tunnel is introduced between the source and the destination and the original path will be deviated.

In WSN since the secure and authentic Multipath Routing Protocol is assumed to be a major challenge which overcomes by Elliptical Curve Cryptography (ECC). It is used to prevent warm Whole attack, maintain secure data transmission and improves the performance of a sensor network by sharing secret keys among nodes in the network. It also improves the overall performance in the network [9]

Now a days an active area of research becoming is, the wireless Sensor Networks (WSNs). They comprise of tiny nodes with limited sensing power, computation and wireless communication capabilities. In the real world applications, the mandatory and primary is considered as the key requirement which has been the success factor of WSN .i.e. the energy efficient ability to provide a communication infra-structure for dissemination of sensed data to a sink node. Thus, a bee-inspired power efficient routing protocol is introduced, Bee Sensor requires little processing and network resources that utilizes a simple bee agent model. In dynamic WSNs scenarios, the Bee Sensor delivers better performance in a as compared to a WSN optimized version of Ad hoc On-demand Distance Vector (AODV) protocol while it’s computational and bandwidth requirements are significantly smaller. It optimizes the energy efficiency, provides scalability, reduces the energy consumption and achieves the better performance in the network [10]

3. Network Model and assumption

In WSN topology, a mobile ad hoc network based system is considered and constructed. A number of 50 nodes are considered with an area of 600m x 600m in a communication range of 250m.

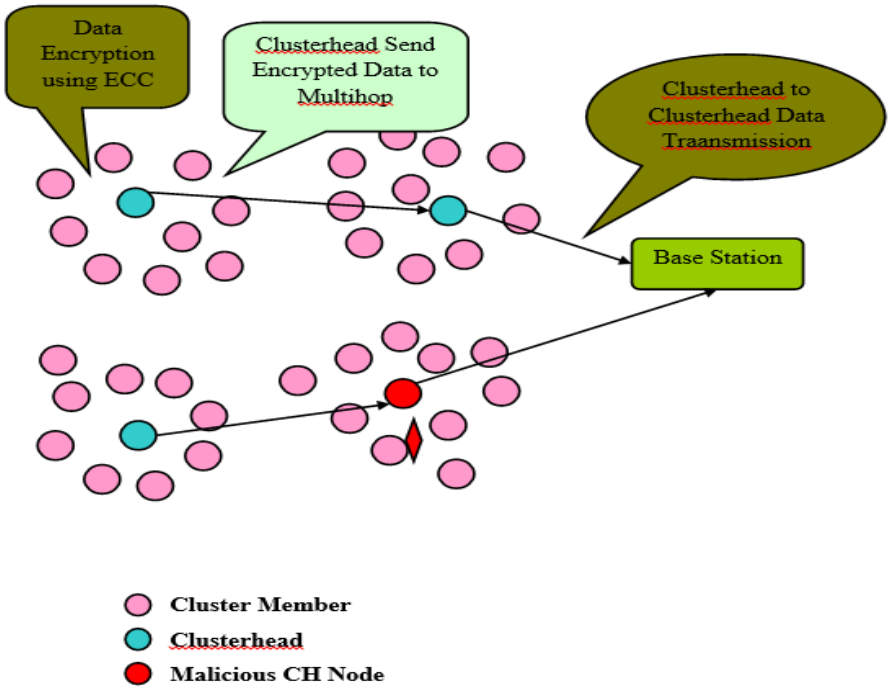


Fig. 1: Network Model Diagram

4. Proposed Work

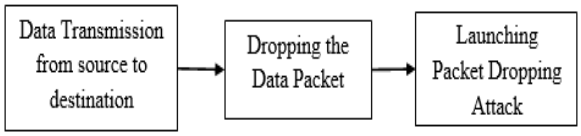
The technique of overhearing by the neighbors is utilized and the packet forwarding statistics are measured by the neighbors such the ratio between the received and forwarded packets to detect black hole attack. If the ratio of packet forwarding is poor it indicates the presence of attack in the network. It leads the identification of alternate path for reliable data transmission.

Thus proposed approach ensures both reliability and data confidentiality.To improve energy efficiency ofrouting energy based CH is used for routing that follows bee colony optimization algorithm.

Fig. 2: Block Diagram

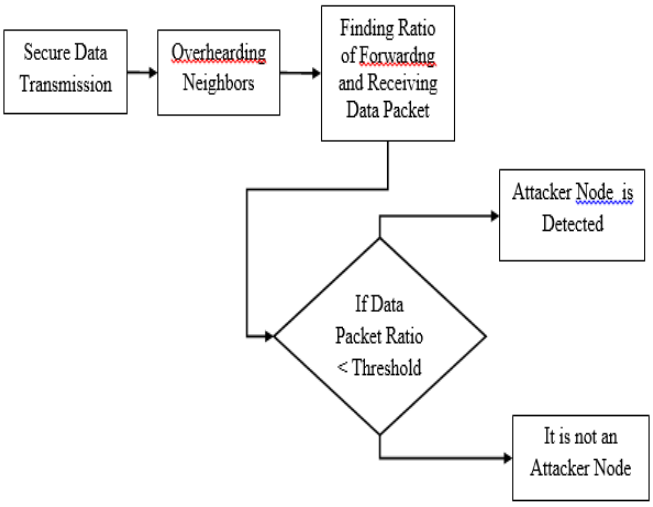
A. Packet Dropping Attack

Input: Data Transmission from Source to Destination
Output: Dropping the Data Packet
Black hole Attack is generally defined as the kind of attack where the attacker node sends a false RREP as an answer to the RREQ and shows itself as a routing node by generating a large sequence number with the freshest route. In this attack the adversary node attracts packets and drops all of them but does not transmit any packet to the destination. Thus due to this attack the packets sent by the nodes does not reach the proposed destination.



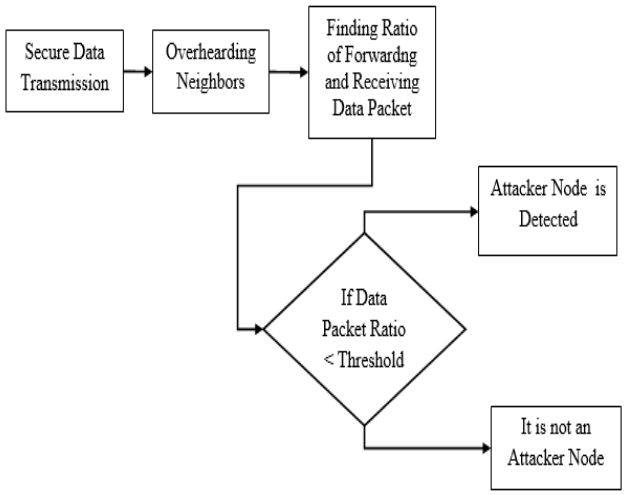
B. Secure Data Transmission using Elliptical Curve Cryptography

Input: Data Transmission from Source to Destination using secure path
Output: Encryption and Decryption
The SC-AOMDV protocol sends encrypted packets from source to the destination by initially discovering the multipath route. The data packet is encrypted using elliptical curve cryptography, as soon as the routing path is discovered from the source to the destination. A secure agent is created that generates the encrypted packet. The packet that is encrypted is initially transmitted from the source to the CH and later from CH to destination. The transmission of the packets is done based on a multi hop manner and reaches the destination based on the best path that is selected among the several multi paths.



C. Black Hole Attack Detection using Overhearing

Input: Packet Forwarding and Receiving
Output: Detection of Attacker using Overhearing
The packet forwarding statistics are measured by the technology of overhearing where all the neighbor nodes hear all the transaction during transmission, such as the black hole attack can be detected based on the ratio between the received packets and forwarded packets. The presence of attack in the network is indicated if there results, in the minimal packet forwarding ratio which leads to the identification of alternate path for reliable and an effective transmission.



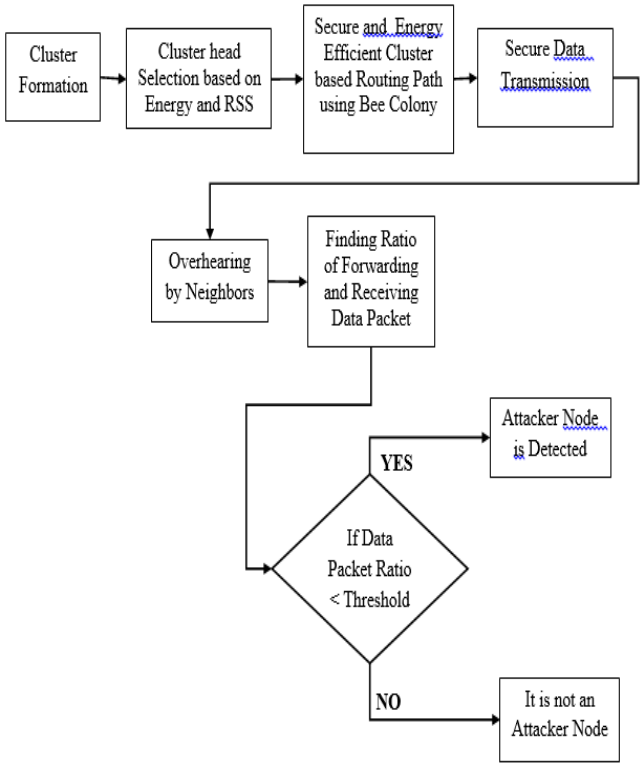
D. Secure Cluster based Routing using Bee Colony Optimization

Input: Clustering Process
Output: Secure andEfficient Routing
Initially during the formation of cluster, all the nodes in the cluster are allocated by a unique ID and a corresponding destination ID. The node that receives hello messages from the surrounding nodes are considered to be in a communication range. Those nodes are considered as neighbors and their IDs are saved in the form of entries in the memory table provided for each and every node. Later the cluster head is selected based on the information attached in the hello message. The selection of cluster head depends on RSS and high energy of the nodes. The node and its neighbors group together for the formation of the cluster.

Scouting
The SC-AOMDV protocol sends encrypted packets from source to the destination by initially discovering the multipath route.

Foraging
The data packet is encrypted using elliptical curve cryptography, as soon as the routing path is discovered from the source to the destination. A secure agent is created that generates the encrypted packet. The packet that is encrypted is initially transmitted from the source to the CH and later from CH to destination. The transmission of the packets is done based on a multi hop manner and reaches the destination based on the best path that is selected among the several multi paths.

On looking
The packet forwarding statistics are measured by the technology of overhearing where all the neighbor nodes hear all the transaction during transmission, such as the black hole attack can be detected based on the ratio between the received packets and forwarded packets. The presence of attack in the network is indicated if there results, in the minimal packet forwarding ratio which leads to the identification of alternate path for reliable and an effective transmission. Thus proposed work assures both reliability and data confidentiality.



Performance Evaluation

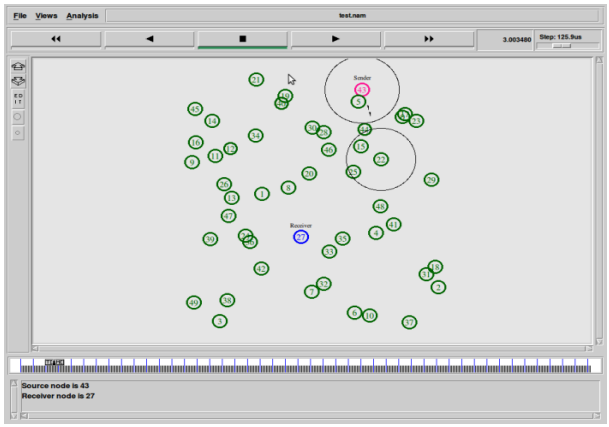
End to End Delay
The time taken for the packet to reach from its source to destination is calculated as the Delay time.
Delay (ms) = ∑ (Delay of each entities data packet) / Total number of delivered data packets

Packet Delivery Ratio
The ratio between the number of packets sent by the source and the number of packets received by the destination is calculated based on the packet delivery ratio. Packet Delivery Ratio = Received Packets / Generated Packets

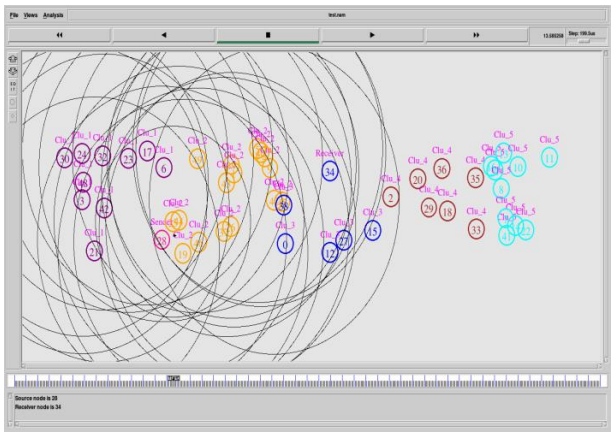
Residual Energy

The residual energy is calculated based on the average amount of energy dwelled from the nodes after certain network operational period.

Data Tranmission



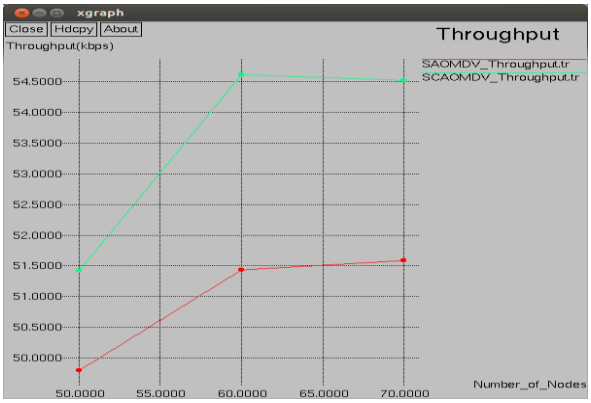
Data Transmission after Cluster Formation



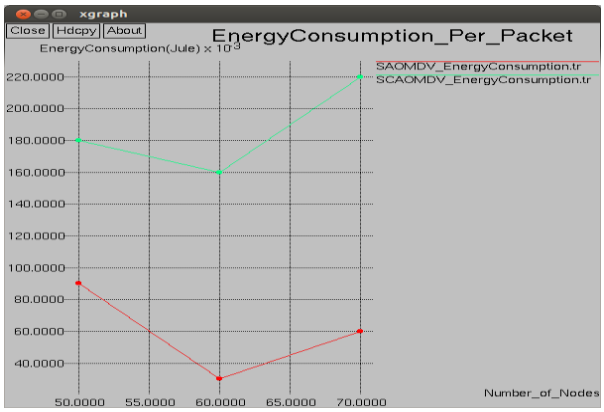
Secure Data Transmission using ECC
Sender = 43
num_nodes is set 50
Source=43 Destination=27
Source's private key = 103
Source's public key Pa = 103*(219, 118) = (51, 199)
Receiver's private key = 205
Receiver's public key Pb = 205*(219, 118) = (39, 218)
Plain Text Message from Source to Receiver: (123) **ECC Message Encryption**
Encrypted Message from Source to Receiver = {Cipher_Text} = {63}
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0

ECC Message Decryption
Decrypted Message from Source = (123)
Source=43 Destination=27
Source's private key = 73
Source's public key Pa = 73*(199, 261) = (134, 234)
Receiver's private key = 145
Receiver's public key Pb = 145*(199, 261) = (33, 27)

Hence the graphical representation is clear comparison of the throughput and the energy consumption per packet. The obtained results have a drastic differentiation between the existing and the proposed work. The effectiveness based on throughput and energy consumption from the proposed work highly excels then that of the existing work.



Graph 1: Demonstration of Throughput



Graph 2: Demonstration of Energy Consumption

5. Conclusions

Existing adhoc routing protocols are subject to a number of attacks that may permit the attacker nodes to effect the selection of routes or to initialize denial-of-service attacks. ECC (Elliptical Curve Cryptography) is integrated with the Bee clustering approach to provide an energy efficient and secure data delivery system. Even though it ensures data confidentiality, data reliability is still disputable such as data dropping attack, Black hole attack (Attacker router drops the data without forwarding to destination). In such cases the technique of overhearing is utilized by the neighbor routers and the packet forwarding statistics are measured based on the ratio between the received and forwarded packets.

References

[1] Bansal Priyanka, Gupta Anuj K, "Impact of Black Hole and Neighbor Attack on AOMDV Routing Protocol", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 3, No. 4, 2014.
[2] Gura, N., Patel, A., Wander, A., Eberle, H. and Shantz, S.C., 2004, August. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In International workshop on cryptographic hardware and embedded systems (pp. 119-132). Springer, Berlin, Heidelberg.
[3] Ghaffari, A., 2015. Congestion control mechanisms in wireless sensor networks: A survey. Journal of network and computer applications, 52, pp.101-115.

[4] Shen, H., He, S., Yu, L. and Sarker, A., 2017, March. Prediction-based redundant data elimination with content overhearing in wireless networks. In Pervasive Computing and Communications (PerCom), 2017 IEEE International Conference on (pp. 50-58). IEEE.

[5] Sett, R. and Banerjee, I., 2015, August. An overhearing based routing scheme for Wireless Sensor Networks. In Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on (pp. 2076-2082). IEEE.

[6] T.C. Camilo, Carreto, J.S. Silva, and F. Boavida, "An Energy-Efficient Ant Based Routing Algorithm for Wireless Sensor Networks", In Proceedings of 5th International Workshop on Ant Colony Optimization and Swarm Intelligence, Brussels, Belgium, pp. 49 - 59, 2006.

[7] Narendra Singh Yadav, Bhaskar P Deosarkar, R. P. Yadav, "A Low Control Overhead Cluster Maintenance Scheme for Mobile Ad hoc Networks", International Journal of Recent Trends in Engineering, Vol .1, No. 1, pp. 1 - 9, 2009.

[8] K Renuka, G. Murali, "Providing Security for Multipath Routing Protocol in Wireless Sensor Networks", International Journal of Research in Engineering and Technology, Vol. 4, No. 2, 2015.

[9] M. Saleem, M. Farooq, "Beesensor: A Bee-Inspired Power Aware Routing Protocol for Wireless Sensor Networks", In M. Giacobini et al. (Eds.), Lecture Notes in Computer Science, Springer Verlag, pp. 81–90, 2007.

[10] Raju M Janardhana, Subbaiah P., Ramesh V., "A novel elliptic curve cryptography based AODV for mobile ad-hoc networks for enhanced security", Journal of Theoretical and Applied Information Technology, December 2013.

[11] Marina, Mahesh K., and Samir R. Das. "Ad hoc onǦdemand multipath distance vector routing." Wireless communications and mobile computing 6.7 (2006): 969-988.