Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 3, Issue 2, 2017
ISSN: 2455 - 7528

Security of Multihop Wireless Network

Mr. Gajanand Sharma, Mr. Ravi Shankar sharma,
JECRC University, Jaipur
gajanan.sharma@gmail.com, er.ravishankarsharma@gmail.com

Abstract :- In this paper, we propose E-STAR for establishing stable and reliable routes in heterogeneous multi-hop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multidimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Analytical results demonstrate that E-STAR can secure the payment and trust calculation without false accusations. Simulation results demonstrate that our routing protocols can improve the packet delivery ratio and route stability.

Keyword:- Wireless Network, MultiHop, NS2, MANET, P2P.

I. Introduction:

Multi-hop wireless networks are the type of networks that require two or more wireless breaks to deliver the information from the source to the destination. From multi-hop wireless network contains more than one intermediate node, there are multiple links that exist between the base station and a definitive system. From multiple paths between source and destination is a significant challenge to find the optimal route out of them. The routing of packets can be defined as the movement of the packets from one host to another through a network, and has been made by devices called as routers. Each intermediate node between the source and the destination is configured with a router and also maintains a routing table. There are several available routing algorithms and depends on the network administrator to select one of them, depending on the nature of the network.

Package is the fundamental unity which contains all the information on the transport within it. The transmission of packets is done using segmentation into smaller segments and then transmit them through a packet-switched network. These packages segmented are transmitted through a network and individually each package you can follow the same path or different. Now, when all sub-packages arrive at their destination, they are reassembled to form a single package.

Types of wireless networks:

This type of wireless networks has two types of applications. They are: [1]

- MANETS
- Multi-hop cellular network

MANETS (Mobile Ad Hoc Networks):MANET is a type of wireless network that require Spanish mobile nods are not connected via any fixed wireless network infrastructure.

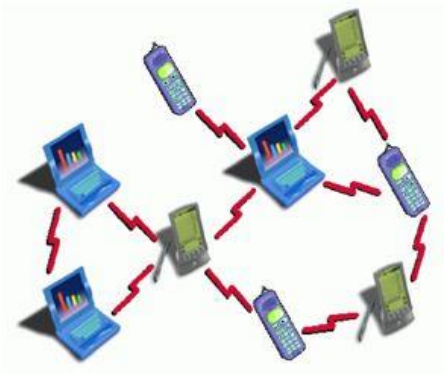


Figure: 1 MANET Network

Instead of obeying any master-slave relationship fixed as cellular system, since the sea remains the direct connection between the nodes or communication is carried out through multiple nodes.

The scope includes: Communication in the field of battle Emergency Call, The public security, etc. Although this network has found its broad applications, there are still some problems that remain unsolved.

Multi-hop mobile network:

Cellular systems usually grant only hops between the base station and the mobile nodes. But the problem that rebound with this type of network is of cell edge

performance that is of great concern. The systems that commitment with the problem are those who have greater carrier frequencies and higher bandwidth. The problem will lead to the loss in path and greater noise attenuation.

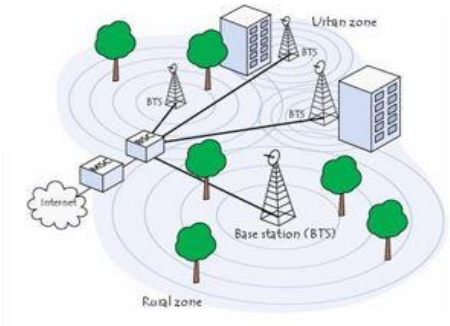


Figure: 2Multi-hop mobile network

Types of relays:
The different types of technologies of relay son:

- Fixed relays: This is a type of relay in technology that is not in the network required to develop the connection.
- Mobile relays: In this type of technology of relay, the relay of mutually users your package.
- Mobile fixed relays: In this technology, the fixed relays are mounted on moving vehicles such as cars, trucks, etc.

II. Literature review:

There are various numbers of researchers who proposed multiple architectures and protocols to protect wireless networks multi-hop. A lot of work has been done in regard to the safety of multi-hop wireless networks. Many researchers have designed new protocols that are designed to provide security for wireless networks multi-hop against various security attacks.

2.1 SECTOR: The sector is one of them. Supports the sector to ensure the monitoring of the node of meetings. Through the sector, any node in the network can try the other nodes are located at a specific time. Srdjan Capkun, Levente Buttyan and Jean Pierre Hubaux successfully presented, a sector which is the mechanism to prevent the wormhole attacks, and thus to secure the routing protocol. The sector is based on the distance, the technique of one-way hash delimiter and claims on trees of Merkle hash. In this document, the set of mechanisms of the UN was proposed for the secure verification of the meetings in multi-hop wireless networks.

2.2 BSMR: A new protocol called as BSMR was proposed by Reza Curtmola and Cristina Nita-Rotaru [2] that can withstand internal attacks the collusion between the adversaries. BSMR is a multicast routing protocol that is based on the software and do not require hardware support. The security of the Protocol BSMR is demonstrated by the results of the simulation.

2.3 shortest path algorithm: Douglas, Daniel, Benjamin and Robert [3] concluded in his work that the shortest path algorithm is not sufficient to increase the performance of wireless networks multi-hop. Following shortest path algorithm does not guarantee the security of the path in the network. The research presented in this work are some experimental settings that demonstrates the insecurity of a minimum number of hops paths with poor performance. Therefore, the shortest path algorithms tend to select the routes that have less capacity than the best paths present in the network.

2.4 ADMR:G. Jorjeta Jetcheva and David B. Joshnson [4] presented the informal design ADMR appraised and protocol. Adaptive Demand-Driven Multicast routing is a routing protocol under demand. Help increase the capacity of the network by reducing the number of components not-on demand within the protocol. In this research, the operation of the Protocol ADMR are described along with the evaluation of their performance.

2.5 Security: Mesh Network:Zhang and Yuguang Yauchao Fang [5] Treaty with success the multi-hop Wireless Mesh Network Security. They also proposed ARSA it is to attack. The flexible security architecture multi-hop Pará Wireless Mesh networks. Wireless Mesh networks is an effective solution of Mayaguez to the ubiquity of broadband internet access. Thus the security of the wireless mesh networks is a major challenge. ARSA help in the limitation of the bilateral agreement between Central Wireless Mesh networks. It also provides the flexibility of delimiter not at any network operator in particular. Instead, users acquire a pass of a third party for universal experience seamless roaming through wireless network of mesh. [6]

- III. Implementation:

The research focuses primarily on achieving Dynamic Source Routing algorithm by designing your modified version and simulation.

A Dynamic Source Routing: DSR Protocol [7] is a type of on-demand routing protocol that is designed for use in wireless network multi-hop. Is legitimate the protocol configuration that eliminates the need to develop a network infrastructure. Source routing is the technique used in the dynamic source routing in place to maintain the tables in each of the

intermediate nodes. The accumulation of direction of addresses of each device between the source and the destination is maintained in order to determine the routes of origin. When the path of the discovery packets are processed, stored in cache addresses accumulated by the processing nodes. Packets are routed with the help of these roads. The packets that are sent contain the address of each device to be paths that lead to the high network overhead and has addresses very large. To overcome this situation, DSR prevents the source routing.

Instead, there is a mechanism in which packets are forwarded in hop-by-hop and maintains a flow of "code them. This Protocol has two phases, i.e. path discovery path and maintenance. Route response message is generated when the package arrives to the desired destination.

The destination node must have the route to reach the source node. The target node could obtain the route from its cache and use it to send the reply message from path. Otherwise, the route saved in the registry of the route is used that is in the message header of the request of route. [8]

Maintenance of route starts when the hay transmission fatal. The path always of the packages of error is generated in the node, the maintenance phase of the path begins to act. Then the erroneous break is removed from the cache and all hops stops at that point. Dynamic Source Routing Protocol (DSR) is a type of protocol on-demand. Deletes messages to update the periodic table stopping the bandwidth consumed by the control of the packages.

Dynamic Source Routing algorithm follows a paradigm in which the path is established by disseminating the path that request packets across the network. The nodes that receives the packet routing request responds with the reply message from Route packet to the source node. [9]

It is based on the following assumptions:

- All nodes in the network participate.
- Do not intervene security issues.
- Network of small diameter (around 10)
- The corrupted and destroyed the packets are detected by the receiver.

At DSR, the mobility of the mobile nodes son moderate when the sending node S has a packet to send ton destination node D, starts a route discovery mechanism to identify a target path. These mechanisms work together to discover and maintain routes in a wireless network. When the path request reaches the destination node, the path is generated the response message. The destination requires a path.

Under certain conditions, unidirectional and selection of tracks to a link can be accepted DSR follows two basic mechanisms:

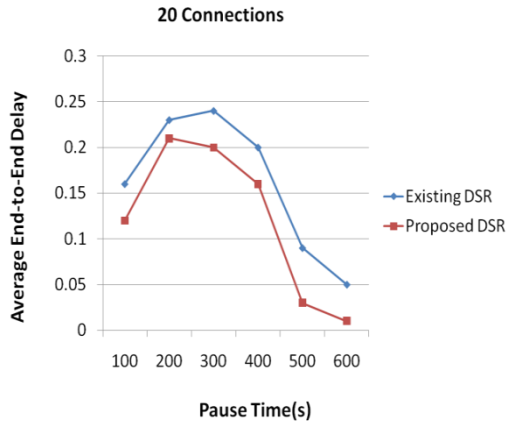
- Path Discovery
- Maintenance of Path Discovery or route record in the message header of the request of routes.

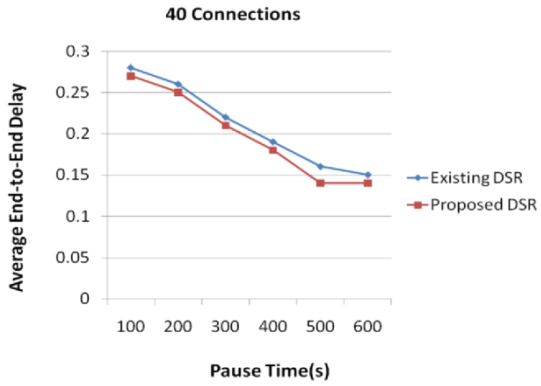
IV. Results and conclusions:

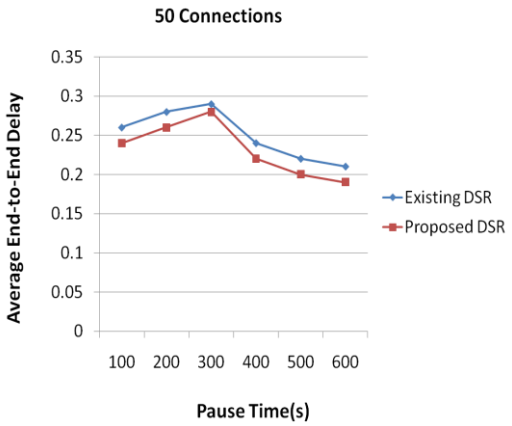
The present study has as objective to modify the algorithm existence and designing a new modified algorithm that has less network overhead, less delay in the transmission of the package and the high quality of network. This study also seeks to compare the modified algorithm and existence in terms of endtoend delay and standardized, loading and delivery of routing packets ratio.

End-to-end delay: End-to-end delay refers to the time it takes the packet to reach the destination node from the source node. [10]

The figures show the comparison of both algorithms when the 20, 40 and 50 connections are present.







V. Conclusion :-

The present study has as objective to modify the algorithm existence and designing a new modified algorithm that has less network overhead, less delay in the transmission of the package and the high quality of network. This study also seeks to compare the modified algorithm and existence in terms of end-toend delay and standardized, loading and delivery of routing packets ratio.

End-to-end delay:

End-to-end delay refers to the time it takes the packet to reach the destination node from the source node. The figures show the comparison of both algorithms when the 20, 40 and 50 connections are present.

References:

[1]. G. Sharma, M. Poonia," Danger Theory Based Model to Prevent Sleep Deprivation Attacks in MANET's," International Journal of Emerging Research in Management &Technology, vol. 4, no. 12, pp. 61-64, 2015.

[2]. F. Michahelles, S. Karpischek, and A. Schmidt, What can the internet of things do for the citizen, IEEE Pervasive Computing, 9(4), 2010, 102–104.

A. Cardenas, S. Amin, and S. Sastry, Secure control: Towards survivable cyberphysical systems, Proceedings of IEEE 28th International Conference on Distributed Computing Systems Workshops (ICDCS), Beijing, China, June 2008, pp. 495–500.

[3]. Y. Zhang, W. Duan, and F. Wang, Architecture and real-time characteristics analysis of the cyberphysical system, Proceedings of IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Xi'an, Shaanxi, China, May 2011, pp. 317–320.

[4]. S. Pandey, M-S. Kim, M-J. Choi, and J. W. Hong, Towards management of machine to machine networks, Proceedings of the 13th Asia-Pacific Network Operations and Management Symposium (APNOMS), Taipei, Taiwan, China, September 2011, pp. 1–7.

[5]. G. Sharma, D. Goyal," A Chronological Review of the Video Streaming Over P2P Networks," International Journal of Computational Research and Development, vol. 2, no. 2, pp. 15-18, 2017.

[6]. M. Starsinic, System architecture challenges in the home M2M network, Proceedings of the Long Island Systems Application and Technology Conference (LISAT), Farmingdale, NY, USA, May 2010, pp. 1– 7.

[7]. G. Sharma, A. Sharma, D. Goyal," Improve Security For Mobile Ad-hoc Networks Using Genetic Zonal Routing Protocol," International Journal of Innovative Science and Research Technology, vol. 1, no. 09, pp. 1-6, 2016.

[8]. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, GRS: The green, reliability, and security of emerging machine to machine communications, IEEE Communications Magazine, 49(4), 2011, 28–35.

[9]. G. Sharma, MK. Jha, RS. Sharma," Performance Evaluation of Quality of Service in Proposed Routing Protocol," Global Journal of Computer Science and Technology, vol. 14, no. 05, pp. 1-10, 2014.