Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 12, December 2015, pg.79 – 87

SECURE COOPERATIVE PACKET SHARING IN MOBILE AD-HOC NETWORKS

S.Srithar[1]
Assistant Professor

Dr. K.Karuppasamy[2]
Professor & Head

Department of Information Technology,
RVS College of Engineering and Technology,
Coimbatore, Tamil Nadu, India
[1]sss.srithar@gmail.com
[2]kps_cse@yahoo.co.in

Abstract— Wireless sensor networks demand networks with high, consistent data load and data protection. For the purpose of content sharing Mobile nodes need to share their information to their neighbor nodes. Transmitting data from the sender node to receiver node through multiple hops need to be secured. For that purpose the sender may follow the secure cooperative content sharing. The content sharing among the nodes in network reduce the data access delay. Here the contents are secured by performing encryption techniques. This encryption technique is handled by using public key management system. In which the sender sends the public key to every nodes in the network the nodes in turn provide the acknowledgement, these nodes are assumed as trusted nodes .The concept of trusted nodes is used to reduce the End-to-End delay between the mobile nodes. The request and response mechanism is further done through the trusted nodes. Once the response is arrived by the sender then it will be recorded in each hop of the transmission path. When other nearest node try to get the same response, the request gets the response by the node from the previous path itself. So there is no need to do the same process repeatedly. By this the time is consumed, the delay in accessing the data is also reduced. Hence by this the contents are shared securely as well as cooperatively in the network. It was implemented by using ns-2 simulation.

I. INTRODUCTION

Mobile Adhoc networks (MANET) is a self configuring infrastructure less networks with mobile devices connected without wires. In MANET the nodes can be in the form of networking devices are it may be mobile devices. All the nodes are act as both server and client, i.e., Peer-to-Peer connection. There are several routing mechanisms are preferred to route the packet from source to Destination. Some routing protocols are AODV, DSDV, DSR etc. Depending upon the application the usage of such protocols

differs. A challenge in mobile ad-hoc network is End-to-End delay, packet delivery ratio, throughput etc. In MANET nodes can move in any direction and no control of it. A very challenge in MANET and other network is mobility. So several parameters are comes in picture.

There are two protocols are commonly preferred for mobile adhoc networks. One is Proactive protocols, in which when the packet needs to be forwarded, it maintains a routing table to route it. Other one is Reactive, which determines a route based on demand. The main key problem in mobile adhoc network is security. Security may violate in any of the seven layers. So we need to provide some encryption technique to send the packet from source node to destination.

II. LITERATURE SURVEY

Heesook Choi, Patrick McDanial, and Thomas F. La Porta[2]proposed and investigated cooperative forwarder node selection mechanism. It is essential because the node should pass the packets from one node to another without any problem of misbehaving with that packet. Privacy Preserving Communication System (PPCS) which applies in all nodes for secure communication. The motive of this research is to error free packet transmission.

George Danezis,Claudia Diaz[1] proposed and investigated the privacy of the node in terms of authentication. In this method the packet is not delivering in same route. It follow different path based on the conditions.

K. Fawaz, N. Abbani, H. Artail [4] proposed and investigated how security is an issue in wireless sensor networks. In WSN the sensing devices can sense the information and send the same to some other node. While sensing lot of sensitive information may be captured from different nodes. It will affect the entire network and cracks the structure of the network.

III. PROBLEM DEFINITION

Assume that if a source node needs a particular data then it sends request to all other nodes to find whether the requested data is available in any of the nodes hence it initially sends a duplicate request to all nodes in the network to find out the nodes that are within the network and the response for duplicate packets is received by the source node after that it sends the original request i.e., the data what the source node actually needs ,then the response is provided to the source node ,by this approach the data transmission is made with use of large number of duplicate packets in the network it leads to overhead traffic and also packet loss of nodes in the network.

Hence to overcome the occurrence of traffic overhead and to avoid packet loss of nodes in the network we are implementing the concept of trusted node which minimize the usage of duplicate packets and so for further transmission there is not an necessity to send duplicate packets again and again to get the response the request –reply transmission can be performed through the trusted nodes. In order to get the response each node in the network were in a need to access same node where the response is available, hence time delay exist in the network.

3.1 OBJECTIVE

To ensure protection of data between the sender and receiver with help of trusted nodes and employ cooperative content sharing. Security is a very dangerous point in mobile communication hence attack can easily be done. To prevent this, authentication is required for sharing the contents securely. In order to send the contents securely a concept known as trusted node is implemented hence once if we find the trusted nodes in the network the forthcoming request, reply transmission can be done effectively by using the trusted nodes itself. To find out the trusted nodes a public key management system is used whereas it performs encryption and decryption of contents by implementing public key cryptosystem technique.

In our system uses RSA algorithm for encrypting and decrypting the location id. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network. Once the source node gets the response from the receiver, the received path will be recorded. When another node try to access for the same data, the sender get the response from the previous path that is recorded in the Query Directory (QD) which reduces the time delay. Hence the contents are shared cooperatively among the network.

IV. SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

MANET's integrates a collection of privacy and anonymity schemes into a coherent solution ,adapted to provide anonymity services to a caching framework .The system composed of caching nodes and directory nodes that communicate among each other according to a particular protocol and hence, adapting the devised solution to the distributed system can be regarded as a contribution. It also proposes a more comprehensive protection framework than a majority of schemes in the literature. The data transmission between the nodes is performed that is if the request data item is not within the local network, a table is formed which

possess the information about all the neighbor nodes in the network such as number of hop counts, distance between each node etc., The objective was to make it difficult for the adversary to locate the destination of packets towards the receiver. To improve receiver privacy, the duplicate packets is used for transmission. The privacy measures are taken until the data is transmitted securely, by the definition of privacy, in addition to data confidentiality, it is also mandatory to achieve communication privacy and privacy of user identity that is to hide the source of a request, the receiver, and any link between them. While the actual contents of the message might be computationally secure via encryption and other techniques to provide anonymity.

4.1.1 DRAWBACKS

- In existing system there was large number of duplicate packets to find the out untrusted nodes.
- For each transmission there was in a need to send the duplicate packets and have to find out the hacker nodes.
- Whenever the transmission takes place the request response mechanism takes time delay due to the large number of duplicate packets.
- For each time they need to find the untrusted node which leads to the delay of transmission.
- In existing system they maintain the Query Directory (QD) separately which may leads to crash the overall networks.

4.2 PROPOSED SYSTEM

Since in the existing system, during the data transmission in the network to send the data's securely there were greater use of duplicate packets to maintain privacy schemes. By the use of large number of duplicate packets for secure transmission leads to over headed traffic which in turn results to packet loss and also delays in the packet transmission. In order to overcome the traffic in the network we come across with the use of a concept known as trusted nodes where we are able to minimize the use of duplicate packets during the data transmission in order to maintain privacy schemes. And also the content is shared cooperatively in which the time delay is reduced.

4.2.1 ADVANTAGES

- It reduces the time delay by minimizing the number of duplicate packets usage, and the content sharing method.
- The data can be protected using the Public Key Management System (PKMS) and RSA Asymmetric Key Algorithm which perform the encryption and decryption process.
- Here when the data shared among the network, for the next time same data can be accessed in the previous transmission path itself not from the server in which the node cooperatively share the contents.

V. SYSTEM DESIGN

5.1 METHODOLOGY

Initially a public key management system is set in the network; this public key management system holds a common public key. The main purpose of this public key management system is to provide a public key for every node in the network. Public key cryptosystem is used for encrypting and decrypting the contents. In this public key cryptography we specify algorithm known as RSA algorithm for encryption and decryption technique as it used for hiding location information which helps to avoid from all types of attacks from outside the network. Public-key, uses two different but mathematically one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. Here we use RSA algorithm for encryption and decryption.

5.2 SYSTEM ARCHITECTURE

Since in the existing system, during the data transmission in the network to send the data's securely there were greater use of duplicate packets to maintain privacy schemes. By the use of large number of duplicate packets for secure transmission leads to over headed traffic which in turn results to packet loss and also delays in the packet transmission. In order to overcome the traffic in the network we come across with the use of a concept known as trusted nodes where we are able to minimize the use of duplicate packets during the data transmission in order to maintain privacy schemes.

Here t1, t2 refers to different timing of the transmission. Here the sender has the PKMS and provide public key to the entire node after identified the untrusted nodes. After getting the key from the sender, all the nodes are ready to get the request and give the response. Then the sender encrypt the request in order to protect from the untrusted node, when the request reaches its destination it decrypt the request and send back the encrypted response. Then the transmission path was recorded. When another node ask for the same response it need not to search for the response from the beginning of the process. It can get the response from the previous transmission path. This activity called as content sharing among mobile ad hoc networks.

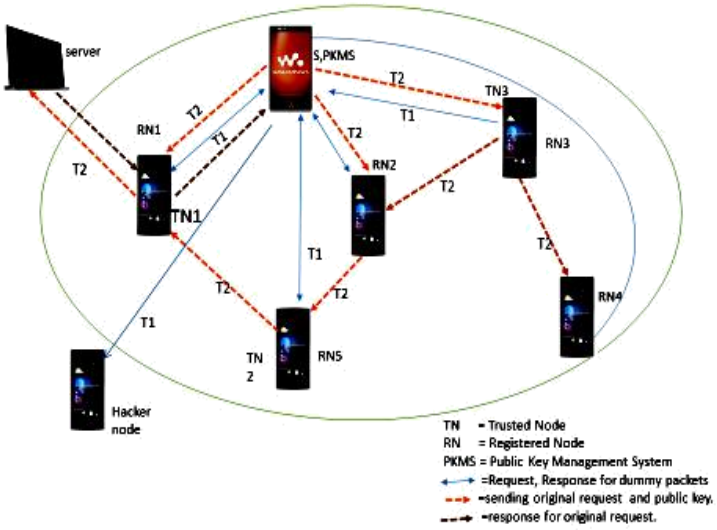

Figure 5.1: Architecture for cooperative content sharing

VI. SYSTEM IMPLEMENATION

6.1 CREATION OF NODES

- The first module defines about the node generation. Initially 10 nodes are created in the network.
- The 10 nodes are created in a network with simulation topology Area is 500x500meter.Here we use the communication protocol as Adhoc On Demand Distance Vector Routing (AODV).This protocol is mainly applicable for avoid link failures, reduce hop-by-hop message exchange, Alternative path selection etc.
- This network uses the MAC standard as IEEE 802.11, the queue length as 1000 packets. It uses the total simulation time as 20 seconds, the simulation starts as 1second.
- The system uses the queue type as Drop tail. The size of the nodes is 40.

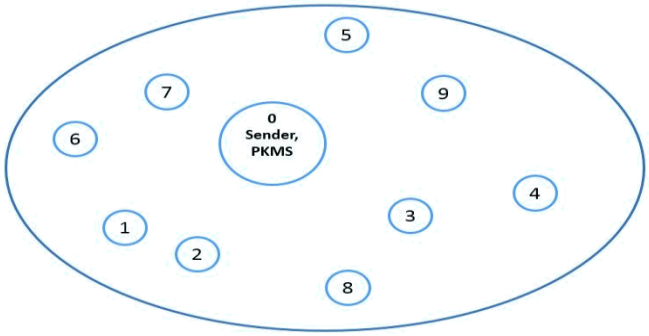

Figure 6.1: Creation of nodes

6.2 BROADCAST DUPLICATE REQUEST

- Broadcast the requests in the network; initially the node is created, in which a source node sends a duplicate request to all other nodes.

- For sending a duplicate request sending we use two traffic types like Transmission control protocol (TCP) and User Datagram Protocol (UDP). The system uses 1000 packets for transmission. It uses the traffic type as CBR.

- After getting the response for the duplicate request the source node sends encrypted request along with the public key to every other node in the network.

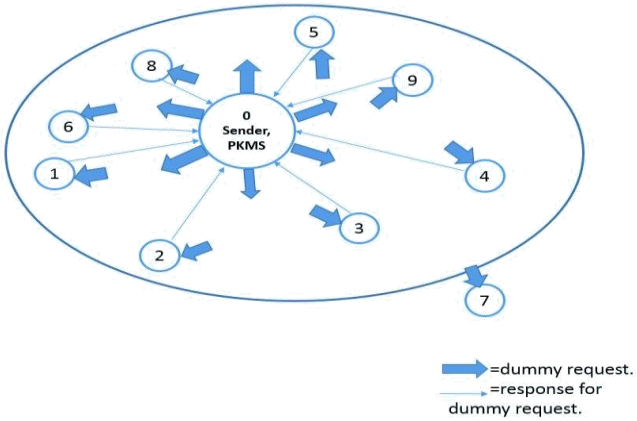

Figure 6.2: Broadcast duplicate request

6.3 IDENTITY MASK ALGORITHM

- The third module defines about implementing the trusted nodes in the network. When the source node needs a data in a network it sends a duplicate request to all other nodes in the network as prescribed in second module, once if the nodes in the network reply for that duplicate request then that nodes are considered as trusted nodes within the network and other nodes that does not provide reply are considered as un-trusted nodes.

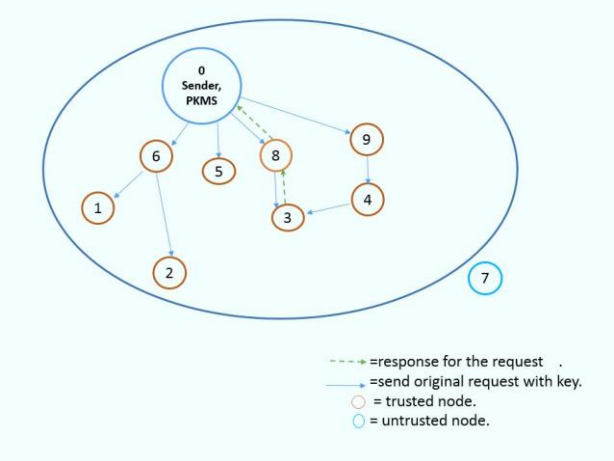

Figure 6.3: Identity mask Algorithm

- Again the source node sends the original request along with the public key to the nodes which are already considered to be as trusted nodes.
- The nodes then reply for the request from the source node by encrypting the original request using the public key and also the individual nodes private key. When the source node receives the response it decrypts the encrypted response and checks outs the correct response.
- RSA (Rivest-Shamir-Adleman) algorithm is implemented for encrypting and decrypting the content. It is the cryptosystem for public key encryption widely used for securing content.

6.4 COOPERATIVE CONTENT SHARING

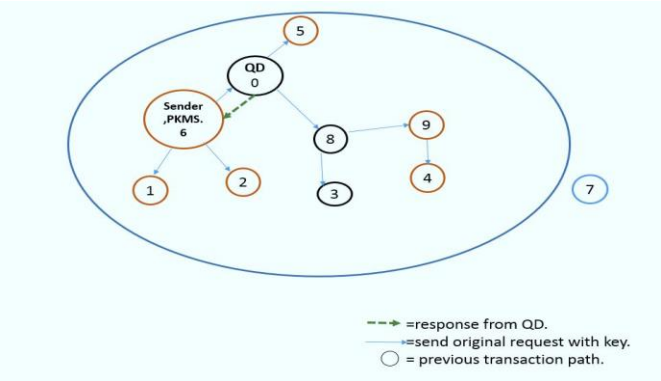

Figure 6.4: Cooperative content sharing

Once the response is arrived from the sender then it will be recorded in each hop of the transmission path. When other nearest nodes try to get the same response, the request gets the response by the node from the previous path itself. So there is no need to do the same process repeatedly. By this the time is consumed, the delay in accessing the data is also reduced. Hence by this the contents are shared cooperatively among the nodes in the network.

6.5 SIMULATION PARAMETERS

S.No	Simulation Parameter	Default Value
1	Simulation Time	20Sec
2	Network Size	500x500m
3	Number of Nodes	10
4	MAC standard	IEEE 802.11
5	MAC data Rate	1Mb
6	Protocols used	AODV
7	Queue Length	1000
8	Simulation Start Time	1sec
9	Traffic Type	UDP,TCP
10	Mobility of nodes	10
11	Packet Size	1000
12	Interval Time	0.1 sec
13	Mobility Type	CBR

Table 6.1 Simulation Parameters

VII. PERFORMANCE ANALYSIS

In our system trace file qos.tr is analyzed and the performance of the Existing system and proposed system is measured and compared by Packet delivery ratio, End-to-End delay.

No.of Nodes	Packet Delivery Ratio	
	Existing Approach	Proposed Approach
10	75	91
20	73	95
30	67	94
40	71	90

Table 7.1 Packet Delivery Ratio

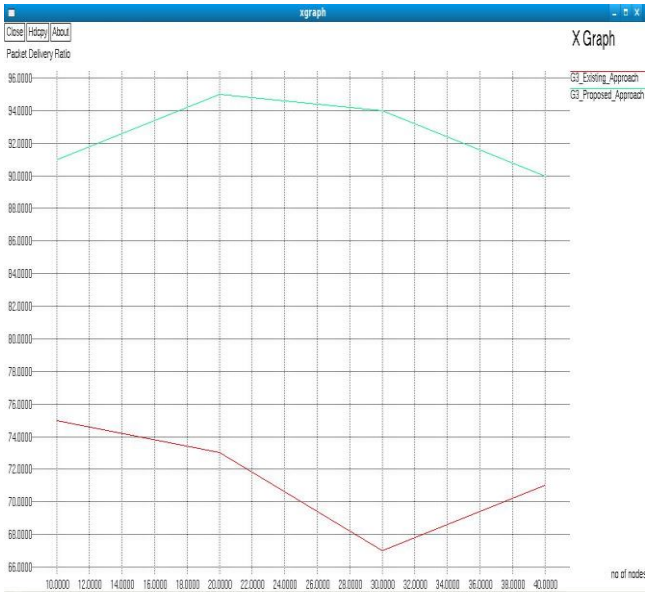

Figure 7.1 Packet delivery ratio graph

Table 7.2 Degree of Anonymity

No.of Nodes	Degree of Anonymity	
	Existing Approach	Proposed Approach
10	.30	.55
20	.25	.50
30	.20	.45
40	.15	.40

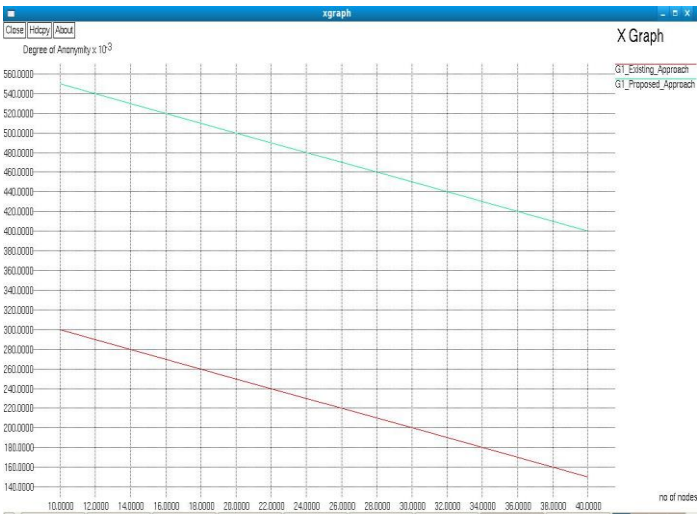

Figure 7.2 Packet delivery ratio graph

VIII. CONCLUSION AND FUTURE ENHANCEMENTS

8.1 CONCLUSION

In our proposed scheme we are minimizing the usage of duplicate packets for data transmission and also to transmit data securely between the nodes in the network. And we overcome the occurrence of traffic in the network by using the concept known as trusted nodes where we are able to minimize the use of duplicate packets during the data transmission in order to minimize time delay.

We use AODV protocol to minimize the packet loss. PKMS (Public key Management System) to provide the public key to all nodes in the network. In Identity Mask Algorithm we use RSA asymmetric key cryptosystem to encrypt and decrypt the location id.

By using this content are shared securely. So the time delay to access particular contents in the network was reduced.

8.2 FUTURE ENHANCEMENT

These mechanisms include request hopping and request piggybacking, where request hopping was used to prevent the local attacker from knowing the exact source of the request while request piggybacking was employed to hide the request event from the global eavesdropper.

For future work, one can look into the possible solutions to achieve high anonymity levels in networks that are characterized with low request activity.

REFERENCES

[1] George Danezis, Claudia Diaz, Towards measuring anonymity, in: Proceedings of the 2nd International Conference on Privacy Enhancing Technologies, 2002.

[2] Heesook Choi, Patrick McDanial, and Thomas F. La Porta, Privacy preserving communication in MANETs, in: IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007.

[3] Jinyuan Sun, Chi Zhang and Yuguang Fang Cooperative caching with adaptive pre fetching in mobile ad hoc networks, in: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, June 2006, pp. 38–44.

[4] K. Fawaz, N. Abbani, H. Artail, A privacy-preserving cache management system for MANETs, in: International Conference on Telecommuncations (ICT), April 2012.

[5] Noor Abbani, Hassan Artail "Protecting Dataflow Anonymity in Mobile Adhoc Networks that employee Cooperative Catching" Ad-hoc networks xxx(2014)xxx-xyz.

[6] P. Kamat, Y. Zhang, W. Trappe, C. Ozturk, Enhancing source-location privacy in sensor network routing, in: 25th International Conference on Distributed Computing Systems (ICSCS'05)

AUTHOR(S) PROFILE

S.Srithar[1] received the B.E degree with honors in computer Science and Engineering and M.Tech degree with honors in Information Technology from PSN College of Engineering and Technology, Tirunelveli, in 2011, 2013.He currently serves as an Assistant Professor in department of Information Technology at RVS College of Engineering and Technology, Coimbatore. His research interests include Mobile computing, Wireless networks, Mobile Ad.hoc Networks, Vehicular Adhoc Networks etc.

K.Karuppasamy[2] received BE degree in Computer Science and Engineering from Mahendra Engineering College, Salem in 2001 and the ME degree in Computer Science and Engineering from Kumaraguru College of Technology ,Coimbatore in 2006.He received the Ph.D degree in WSN from Anna University, Chennai in 2013.He has 13 years of experience in teaching. At present he is professor & Head in Department of IT at RVS College of Engineering and Technology, Coimbatore. His research focus on wireless sensor networks, MANETs, mobile computing, cloud computing etc.

