International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.04, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Dynamic and secure transmission in multihop communications

I. RAVIKUMAR[1], M. JAMES STEPHEN[2]

Assistant Professor[1], Professor2

[1,2]Dept of CSE, WISTM ENGINEERING COLLEGE, PINAGADI, VSP, A.P

ABSTRACT

We propose a novel dynamic network control of secure transmission between multiple nodes in multi hop communications. Even though model proposed by various authors from years of research, every model has its own advantages and disadvantages. In this paper we propose we propose a secure cluster based secure transmission with trust metrics for path computation between the source and destination and simple encoding model for data encoding and data encoding between the end points and cluster based node communication improves the performance. Our proposed model gives more efficient results than traditional models.

I. INTRODUCTION

MANET can be represented by a weighed graph G(V, E) where V is the set of nodes in the network and E is the set of links with connected nodes which are in transmission range of each other. Since V and E change with the moving, joining and leaving of nodes[1][2], MANET has a dynamic topology. Each node has a unique identification as well as one sender and one receiver at least. Assume that each node has the same transmission distance. If two nodes are within the transmission range they are regarded as neighbors and there is a link between them. Each node cyclically sends message to get its neighbor set. Adjacent nodes share the same wireless media and transmit messages through local broadcasting. Considering the faulty nature of MANET, constructing the route that meets the bandwidth requirements while also meeting certain reliability requirements would result in better performance. Given the minimum bandwidth and reliability requirements Bmin and Rmin, the QoS routing problem from source node S to destination node D is to find the feasible paths which satisfies Bandwidth(P)≥Bmin and Reliability(P) ≥Rmin. While there are a number of such paths, we choose N paths amongst them as the multipath routing. The ideal value of N will be determined in next section to achieve the compromising between load balancing and network overhead[4].

Usually every model transmits the data packets from source to destination through various intermediate nodes with losing the integrity and confidentiality. Data packets cannot be transmitted between the source and destination nodes; it involves various intermediate notes, base stations and mobile terminals and followed by proxies. Proxies improved performance by reducing other overhead to the centralized servers. Centralized server

maintains the multiple servers to handle the multiple requests synchronously and without losing the reliability [3].

In find the path between the source mobile terminal to destination mobile terminal , it needs to identify the various paths and factors which chooses the intermediate nodes. If we can consider all set of nodes it is very complex in terms of path computation. Cluster based models improves the performance by excluding the unnecessary intermediate nodes in path computation. Cluster based models groups the similar set of nodes which are useful in path computation [5].

II. RELATED WORK

To achieve the data confidentiality our model proposed an efficient and dynamic end to end data encoding and decoding model between two end points. Data packets can be transmitted in terms of blocks . Every block individually encoded and decodes at the receiver end and transmitted through the intermediate nodes without losing the data integrity ad confidentiality [6].

In multihop network communications , every intermediate node possibly overhears the data transmission of a data packet many times as it is transmitted over different intermediate nodes. We consider such integration of information over multiple transmissions. Thus, we need to go beyond the scenario in which the paths are disjoint and each intermediate node has only one path crossing[7].

The problem of network control with confidential messages has been studied (as shall be discussed in the next section), in the

past for the single-hop setting. The main additional challenges involved in generalizing this problem to multihop networks are dynamic end-to-end encoding and multipath routing. Standard

dynamic control algorithms give control decisions in each time slot independently by assuming time-scale separation, i.e., independent transmissions of subsequent slots [8]. The confidential message is encoded across many blocks, which implies that the time-scale involved in physical-layer resource allocation cannot be decomposed from the time scales involved in network-layer resource allocation, eliminating the time-scale separation assumption of standard dynamic control algorithms. A similar problem was previously addressed in [9], where the users leave (arrive) the system, e.g., whenever their queues empty (has one packet arrival). However, the network makes a control decision only at the slot boundaries, delaying the network response for at most one slot duration. On the other hand, in our system, due to the encoding of the confidential messages into many blocks, the network decisions made at every slot become dependent with each other. This poses new and fairly different challenges in addressing the separation of time scales. Here, in order to design a cross-layer dynamic control algorithm, source needs to keep track of the rate of information obtained by each intermediate node during the transmission of encoded confidential message, and this information is required to be quantified over each time slot independently. In addition, the existing schemes for wireless multihop networks are not concerned with how information ought to be spatially distributed in the network [10]. Additional “virtual”

queues need to be maintained to keep track of the leaked information to other nodes in the network to make sure that information from the source node is sufficiently spatially distributed in the network. Hence, unlike the standard multihop dynamic algorithm where the objective is to only increase
end-to-end flow rates, in our problem, increasing the flow rate and keeping confidentiality of the messages appear as two conflicting objectives.

III. PROPOSED WORK:

We propose an empirical model of trust based transmission gives optimal route computation with mutual trust and indirect trust .Every node has trust metrics which helps to identify the genuine nodes as a factor of measurement .Cluster based implementation groups the set of nodes based on the trust factor and data can be transmitted securely. We design a novel network access model which improves the network communication between the nodes. Cryptographic model securely encodes and decodes the data between the source and destination nodes during the communication.

In Secure access networks, central stations are the nodes which can receive and send data to or from other base stations through input and output terminal. Set of base stations can be connected to input and output terminals. All mobile terminals can be connected to data center. Data center data storage area can hold the data packets which are received from mobile terminals. Mobile or sender / receiver are the users can receive signal from base stations. Multiple virtual proxies can be attached to mobile terminal to minimize additional overhead. In proposed design architecture every request from base station can be forwarded to mobile terminal, in turn it redirects the request to mobile proxy. It is not possible in traditional approach.

Clustering is an implementation which helps in grouping the similar type of objects or nodes. Instead of simple labeling of nodes, we cluster the nodes based on signal mutual trust and indirect trust to group optimal cost based clusters. Initially centroids can be selected and cost can be computed and compared with node with respect to all centroids and place the node in optimal centroid or cluster ,repeat the same process until all nodes are processed and this process can be done iteratively up to nu number of iterations.

1: Select K points as initial centroids for initial iteration
2: until Termination condition is met (user specified maximum no of iterations)
3: Measure the cost interms of mutual trust and indirect trust
Cost :=Mutual trust + indirect trust
4: Assign each point to its closest centroid to form K clusters
5: select a new centroid from the cluster and start from step3
6: stop and return clusters

Data can be securely transmitted through data centers between nodes with vector model mod encoder technique. Instead of traditional model of cipher conversion, it converts the entire user data to quotient and reminder vectors with respect to delta value.

➢ **MOD-ENCODER Encoding Algorithm:**

- Input : M ∈∑, Δ value
- N=|M|, i.e length of M
- Z=n * bit size, i.e bit size is the number of bits require to represent each character
- For i=1 to n
  - Read m_i the i^{th}character from M
  - Find R

$$R[I]=I(m_i)\%\Delta$$

  - Find Q

$$Q[I]=I(mi)/\Delta$$

- Representation of R
  - For I=1 to n
  - Represent R[I] in base Δ
- Representation of Q

➢ **MOD-ENCODER Decoding Algorithm:**

- Input : Bi-tuple <R,Q>, Δ value
- Let QB=(q1,q2,….qn) be the representation in Base B
- Interpret R as a vector of Base Δ number
- For $1 \leq i \leq n$
  - $I=qi \times \Delta + ri$

Where qi the ith digit of QB,ri the ith element of R.

- Mi=I-1(i)
- M=(m1,m2,….mn)

The encoded message is a bi-tuple of which, the first is a vector of quotients denoted as Qand the second is a representation of remainders denoted as Rwith respect to a modulus M. The secrecy of the message is retained by communicating Rover a secure channel using some standard encryption mechanism. The computation overhead is also reduced as the encryption is done only on one half of the encoded message

Conclusion:

We have been concluding our current research work with efficient design architecture through base station and mobile nodes. Initially request made from the source node and transmitted through intermediate nodes and base station through mobile terminal. Receiver end nodes can be clustered based on the trust factor and generates the set of nodes and search for the destination node. Our implementation gives more efficient results than traditional models.

REFERENCES

[1] S. Murthy and G. L. Aceves, "An Efficient Routing Protocol for Wireless Networks," Mobile Networks and Applications, 1996, Vol. 1, No. 2.

[2] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proceedings of ACM SIGCOMM, 1994, pp. 234-244.

[3] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[4] D. B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, 1996, pp. 153-181.

[5] S. Mueller, R. P. Tsang and D. Ghosal, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges," In Performance Tools and Applications to Networked Systems, Vol. 2965 of LNCS, 2004

[6] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[7] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[8] O. Gungor, J. Tan, C. E. Koksal, H. E. Gamal, and N. B. Shroff, "Joint power and secret key queue management for delay limited secure communication," presented at the IEEE INFOCOM 2010, San Diego, CA, USA, Mar. 2010.

[9] A. Khisti and G. W. Wornel, "Secure transmissions with multiple antennas: The misome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3014, July 2010.

[10] S. Shaffiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of gaussian mimo wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.