6th International Conference on Science, Technology and Management
India International Centre, New Delhi (ICSTM-16)
04 December 2016 , www.conferenceworld.in ISBN: 978-93-86171-16-0

A ZONE ADAPTIVE TRUST EVALUATION METHOD FOR SECURE COMMUNICATION IN MOBILE NETWORK

Milan Singh[1], Deepak Sinwar[2]

[1]*PG Student, Department of Computer Science,*
BRCM College of Engineering and Technology, Bahal, (India)
[2]*Assistant Professor, Department of Computer Science,*
BRCM College of Engineering and Technology, Bahal, (India)

ABSTRACT

A mobile network is public and dynamic network that provides the cooperative route formulation for communication. The open access network allow to any node to participate in the network as a forwarder. In this research work, a dual featured model is provided to perform the safe communication in critical mobile network. The proposed model is able to provide the safe communication under some internal and external attacks. The RSA based authentication is applied to perform the safe selection on selected path nodes. Only the effectively selected nodes can act as an intermediate node for safe route formation. The presented work model is simulated on random mobile network in NS2 environment. The comparative results show that the proposed method has reduced the communication loss and improved the packet communication over the network.

Keywords*: *Encoded Communication, Mobile Network, Reliable, RSA, Trust.

I INTRODUCTION

A mobile network is the open area network without specification of any fixed infrastructure. The dynamic selection of cooperative nodes is done to generate the communication path between the node pairs. The network suffers from various internal and external attacks. The dynamic nature of the network increases the criticality of the network. This dynamism exists in terms of changing node position, inclusion of new nodes as well as selection of different routing path.

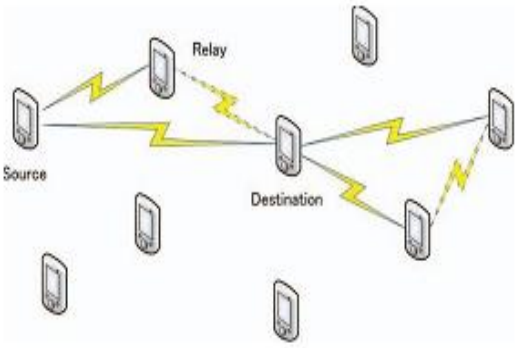

Figure 1: Mobile Network

As the network having different kind of communication in terms of different data and media forms. The security is the primary criteria for reliable communication in mobile network. The network speed, data size, mobility are the factors that affects the communication in mobile network. The environment can be indoor or outdoor where communication can be performed. The architecture adaptation communication can be provided to generate the effective cooperative connectivity so that the reliable communication within the session will be performed. A typical mobile network is shown here in figure 1. Some of the criticalities of mobile network are defined here under:

A) Security

The open access and public available distributed network always having the problem of intrusion at different level. The validated communication is required to improve the communication reliability. There are number of detection based, authentication based and preventive methods to provide security against different kind of attacks. The authentication methods are basically used to verify the node identity and to recognize the intruder with false identity. A node which has proven its identity can be checked under some attack specific detection method or the preventive measure to provide secures communication. The attack specification and relative secure communication is required to reduce the communication loss and information theft.

B) Reliability

The network not only suffers from various attacks but also affected by various communication relative challenges. These challenges include the heavy communication performed in the network. The challenge impurities, sharing and the other channel aspects can also results the communication. Any kind of communication fault, channel failure, lack of synchronization can also result the communication failure. The node level and network level strength analysis can be performed to achieve the communication reliability. The parameter specific observations can be done based on the various possible criticalities such as loss rate, delay, response time etc. Once all the considerations are mapped, the safe and reliable communication can be obtained for the network.

C) Instant Connectivity

Cooperative communication nature is the main property of mobile network. The network provides the dynamic route formation and instant connectivity to generate the effective path. Such kind of connectivity comes under on-demand routing method so that the effective communication path will be formed over the network. The configuration and localization independent connectivity list is generated for each node and under the effectiveness estimation; the route formation can be done. The method is able to store the connectivity in the form of table so that the connectivity time or the response time will be reduced. There are number of methods to form such connectives and to generate the effective communication in the network.

D) Communication Architecture

Another criticality of mobile network is the communication architecture relative to which the communication scenario can be setup. To generate the effective route or communication, the first requirement is to adapt the network features. The network environment or architecture can be captured with current requirement and behavior to perform he communication. Various considerations are taken in terms of zone formation, connectivity observation, environment analysis, channel specification are the key criteria considered while

evaluating the architecture. The group specific or the cluster specific communication is also considered to improve the communication. The node level tracking along with the communication characterization is also provided to generate the safe and reliable communication.

E) Route Recovery

The route recovery is defined to provide the safe communication if some failure occur. The stability of the route is provided to generate the communication. At the earlier phase, the neighbor list can be generated and relatively fault specific communication can be performed. The network disruption and coverage analysis can be performed to identify the node failure or the link break. Based on these requirements, the trust analysis for the communication route formation can be done.

In this paper, an effective dual safety based secure communication model is provided for mobile network. The method has used the authentication inclusive and zone adaptive trust evaluation approach for effective communication in mobile network. In this section, various criticalities for mobile network are identified. The various causes of communication loss that can occur in a network are identified. In section II, the proposed work model is defined with algorithmic specification. In section III, the results obtained from the work are provided. In section IV, the conclusion obtained for the work is presented.

II RELATED WORK

Mobile network suffers from various internal and external attacks because of its dynamic nature. Lot of preventive and detection based methods are provided for secure communication against these attacks. A study work on various security attacks and its improvement to the routing protocol was discussed by K. Singh et. al., [7]. Author defined improvement over the existing protocol against various protocols including Rushing Attack, Flooding Attack etc. S. B. Sharma et. al., [14] has identified the various security issues and relative solutions for mobile network. The malicious node detection and communication using cryptographic method is provided. The position and trust based methods are also described in this paper. Another work on threat identification and communication in mobile network by M. M. Alani et. al., [16]. Various methods to mitigate the attack risk is also provided in this paper. Another analysis on security attacks and attack detection method for mobile network was provided by P. Rajakumar et. al., [23]. The attack specific algorithmic approach is defined in this paper.

One such criteria for optimizing the communication in attacked network is trust analysis. V. S. Bhargavi et. al., [1] has defined a trust based secure routing in mobile network. The neighbor node analysis was provided based on the history transaction to identify the trustful nodes in the network. Another work on association and mobility analysis based trust analysis method was defined using D. Q. Nguyen et. al., [4]. The mobility analysis based trust model is defined to generate the delay component analysis for parameter specific evaluation. The accuracy concern based secure handshaking is performed and relatively route formation is done. A work on Trust Negotiation was provided for enforcing the secure routing mobile network. The delegation adaptive trust modeling is provided to generate the safe route in mobile network. A. B. C. Douss et. al., [10] has defined the validation and specification based trust management scheme for secure route formation for mobile network. The cluster specific trust evaluation was provided under the communication semantics. The consistency and completeness are the key factors analyzed by the author to generate the effective route. S. Sirehka et. al., [15]

has defined an unified trust management scheme to improve the communication against uncertain reasoning. The Bayesian inference theory is defined to observe the nodes and to generate the routing path based on the trust evolution. The quantitative measures are defined to improve the communication in mobile network. A. B. C. Douss et. al., [19] has provided a secure communication under Collusion attacks in mobile network. The delegation specific secure communication is provided to improve the network functionality and damage control.

To provide the data safety against internal attacks and identity specific attack, different authentication specific and encryption specific methods are provided by the researchers. P. D. Nikam et. al., [2] has defined a secure communication using Elliptic Curve Cryptography method. The key generation and key specific communication is provided to maintain the data integrity. E. E. Zakaria et. al., [5] has defined the work to improve the access control for auto configuration networks. The identity based cryptography method and trust management is defined. The QoS analysis was applied to control the node access in the coverage region and relatively secure communication will be performed. D. Suvarna et. al., [6] has defined the secure acknowledgement mapping using digital signature and clustering algorithm. The emergency recovery based acknowledgement observation was provided to identify the misbehaving nodes. Based on the key mapping, the secure communication path is generated. A work on block encoding to improve the security in mobile network was provided by S. J. Ahmad et. al., [12]. The block cipher is applied on packet header and relatively secure security block based communication is provided to reduce the computation and to improve the communication in mobile network. S. R. M. Krishna et. al., [13] has finger print preserved cryptography model is defined for secure communication in mobile network. The key specific encoding method is provided for secure communication in mobile network. K. T. Selvi et. al., [18] has defined an optimized routing model using encoding technique. The security measure based interpolation method is defined to generate the compromised path in mobile network. The topology control based communication and routing in mobile network is provided in this work. A. Echchaachoui et. al., [22] has used the asymmetric and dynamic encoding method to improve the routing reliability for mobile network. The secure and reliable communication was provided to improve the traffic encryption for mobile network. The attack preserved communication method was provided to improve the reliability and security in mobile network. K. S. Dhanalakshmi et. al., [24] has provided a hybrid method for key generation and secure communication in mobile network. The model used the watch dog integrated instant key generation method to improve the data security in mobile network.

Some of the researchers defined attack prevention and avoidance in mobile network. V. G. Mohite et. al., [3] has defined an agent based avoidance algorithm to provide secure communication against black hole attack. The agent specific route forward attack defined for alert notification and relatively provided the cross checking on attack. M. N. Bhargavi et. al., [8] has used the Random key based sharing method to generate the alternative route in mobile network. The online key inclusive threshold limit is applied to generate the adpative safe route. S. Shalini et. al., [9] has defined the random key based compromise path formation in mobile network. The target nodes specific neighbor node analysis was provided to provide reliable route formation in mobile network. The node specific validation is applied for reliable route formation in mobile network. A distributed policy driven evaluation method to observe the node behavior so that the secure communication will be drawn in the network. The neighbor node evaluation is provided under the trust policy rule specificaiton so that the

reliable communication is provided. A qualitative and functional model for secure mobile communication is provided by S. V. B. Rakas et. al., [17]. The proposed method improved the network under resource distribution, QoS management and secures transmission. A. S. Kumar et. al., [20] has defined a work on HMAC protocol for secure communication in mobile network. The symmetric key basd handshaking is provided to identify the valid trusted node and relatively generated the compromised path. The method improved the communication reliability for the network. A time stamp based secure communication in mobile network and it is provided by G. Kulkarni et. al., [21]. The eavesdropping analysis, effective authentication and secure communication is provided by the author under time stamp observation. The neighbor table based secure communication was provided to improve the information exchange in mobile network.

III RESEARCH METHDOLOGY

In this work, an improved trust model based cryptographic method is included to improve the strength of mobile network. The work is here divided in three modules:

- At first, the mobile network will be divided in smaller zones. These zones will be generated in the network with specification of some controller and the relative node specification.
- At second level, the analysis on each zone will be provided under different communication criteria. The features considered here include node stability, communication delay, node degree etc.
- Finally, the categorization of trustful and untrustful nodes will be done. The RSA cryptography algorithm will be applied to allow the untrustful and new nodes. The inter-group communication can be performed directly whereas the intra communication will be implied via the key adaptive encoding.

Because of this there is the requirement of some method that can provide more trustful route generation method under mobility and network reconfiguration situations. The proposed zone trust based encoding model will provide effective and reliable route formulation for mobile network. The evaluation on trust on each zone is done with parameter specification. The algorithmic specification presented in this work is given here in table 1.

Table 1: Trust Based Route Formation Algorithm

Algorithm(MNodes, MSrc,MDst) /*MNodes is the list of mobile nodes in the network with specification of source and destination node */ { 1. Set Cur=MSrc [Initialize the communication on Source node Setting it as current node] 2. While(Cur<>MDst) [The route will be formed till the destination node not occur]

{

3. Znodes=GetZoneNodes(Cur)

[Divide the network in smaller zones under coverage specification and identify the coverage nodes]

4. Zweights=TrustEvaluate(Znodes)

[Perform the Trust Evaluation on zone nodes under connectivity, lossrate and delay parameters]

5. Enode=GetEffectiveNode(Zweights)

[Based on trust evaluation identify the most effective communication node]

6. Path=[Path Enode]

Cur=Enode

[Set Effective weighted node as current node]

}

7. Set the Communication path

8. SPath=RSAVerification(Path)

[Apply the authentication for node level validity]

9. PerformCommunication(SPath,Src)

[Perform Communication over the path]

}

Here table 1 is showing the proposed algorithm to generate the communication route under trust evaluation. The algorithm shows that the network is first divided in smaller zones and for each zone, the trust evaluation was performed. The trust evaluation is done based on the coverage, communication and communication delay parameters. By identifying the most trustful nodes in each zone, the effective route is formed in the network. The presented work is implemented in NS2 environment. The results obtained from the work are provided in next section.

IV RESULTS

A mobile area network network is one of the most complex networks as it is network with cooperative communication. To perform the complete work we have taken a indoor scenario in NS2. In this work a trust adaptive analysis is provided to control the network communication. The network scenario defined for the work is shown in table 2.

Table 2: Network Scenario

Parameter	Value
Network Area	100x100
Total Nodes	25
Protocol	AODV
Mac Protocol	802.11
Simulation Time	100ms
Topology	Random
Mobility	Random
Propagation model	Two ray ground
Antenna Model	Omni directional
MS Speed	Random

The defined parameter shows that the trust based communication is performed in a limited network with 25 nodes. The AODV routing protocol is defined and the analysis is performed in terms of packet communication and communication loss parameters. The comparative analysis in terms of packet communication is shown in figure 2.

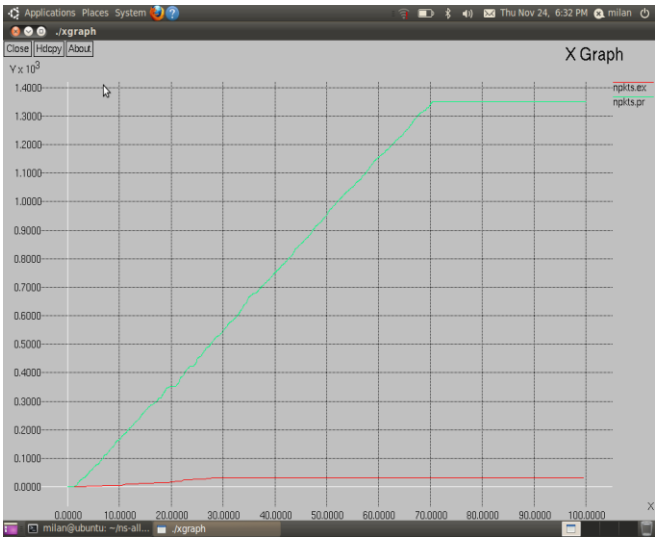

Figure 2: Packet Communication (Existing Vs. Proposed)

Here figure 2 is showing the packet communication analysis in case of existing and proposed work. Here x axis shows the simulation time and y axis is showing the packet communication. The simulation results show that the method has improved the packet communication.

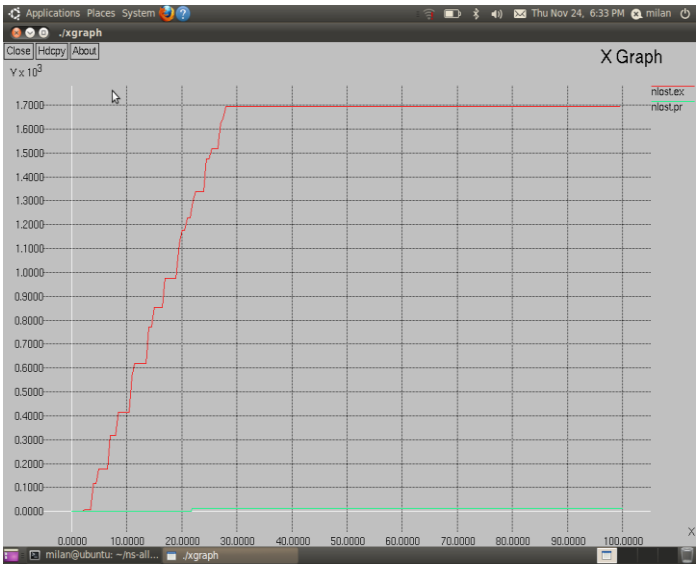

Figure 3: Packet Loss (Existing Vs. Proposed)

Here figure 3 is showing the packet loss analysis in case of existing and proposed work. Here x axis shows the simulation time and y axis is showing the packet loss over the network. The simulation results show that the method has improved the packet loss.

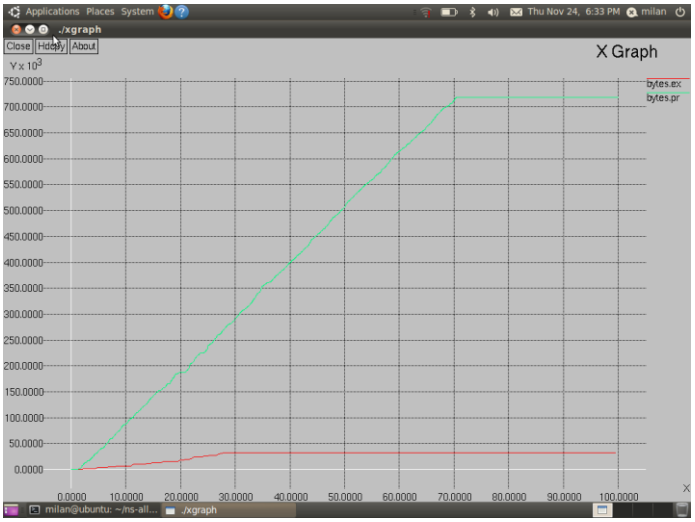

Figure 4: Bytes Communication (Existing Vs. Proposed)

Here figure 4 is showing the bytes communication analysis in case of existing and proposed work. Here x axis shows the simulation time and y axis is showing the bytes transmission over the network. The simulation results show that the method has improved the bytes communication.

V CONCLUSION

In this paper, a dual safety based secure communication method is provided for reliable communication in mobile network. At the early stage of this model, the network is divided in smaller zones and for each zone, the trust evaluation is done on each node. Based on this trust analysis, the route is generated over the network. The

work model is implemented in NS2 environment. The results show that the method has improved the communication and reliability.

REFERENCES

[1] V. S. Bhargavi and S. V. Raju, "Enhancing Security in MANETS through Trust-Aware Routing," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1940-1943.

[2] P. D. Nikam and V. Raut, "Improoved MANET Security Using Elliptic Curve Cryptography and EAACK," International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, 2015, pp. 1125-1129.

[3] V. G. Mohite and L. Ragha, "Security Agents for Detecting and Avoiding Cooperative Blackhole Attacks in MANET," International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, 2015, pp. 306-311.

[4] D. Q. Nguyen, M. Toulgoat and L. Lamont, "Impact of Trust-Based Security Association and Mobility on the Delay Metric in MANET," Journal of Communications and Networks, 2016, vol. 18, no. 1, pp. 105-111.

[5] E. E. Zakaria, H. S. Hamza and I. A. Saroit, "An Integrated Security Framework for Access Control and Address Auto-Configuration for MANETs," 8th IFIP Wireless and Mobile Networking Conference (WMNC), Munich, 2015, pp. 253-260.

[6] D. Suvarna, E. Pallavi, L. Sumitra, D. Chhaya and M. Korade, "Acknowledgement Security for MANET using EAACK," International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 671-678.

[7] K. Singh, A. Boparai, V. Handa and S. Rani, "Performance Analysis of Security Attacks and Improvements of Routing Protocols in MANET," Second International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM), Lodz, 2015, pp. 163-169.

[8] M. N. Bhargavi, C. Naikodi and L. Suresh, "Sharing Randomly-Generated Keys via Alternative Route in a Threshold Based Path Oriented Network for Robust Security in MANETs," International Conference on Advanced Computing and Communication Systems, Coimbatore, 2015, pp. 1-6.

[9] S. Shalini, C. Naikodi and L. Suresh, "Path Oriented Randomly-Generated Keys for Uncompromising Security in MANETs," International Conference on Advanced Computing and Communication Systems, Coimbatore, 2015, pp. 1-6.

[10] A. B. C. Douss, S. Ayed, R. Abassi, N. Cuppens and S. G. E. Fatmi, "Trust Negotiation Based Approach to Enforce MANET Routing Security," 10th International Conference on Availability, Reliability and Security, Toulouse, 2015, pp. 360-366.

[11] A. Tajalli-Yazdi, H. Lutfiyya and D. Kidston, "MANET Security through a Distributed Policy-Based Evaluation of Node Behaviour," International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, 2015, pp. 923-928.

[12] S. J. Ahmad and P. R. Krishna, "Security on MANETs using Block Coding," International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, 2015, pp. 2054-2060.

[13] S. R. M. Krishna, P. V. K. Prasad, M. N. S. Ramanath and B. M. Kumari, "Security in MANET Routing Tables with FMNK Cryptography Model," International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, 2015, pp. 1-7.

[14] S. B. Sharma and N. Chauhan, "Security issues and their solutions in MANET," International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Noida, 2015, pp. 289-294.

[15] S. Sasirehka, S. Vijayakumar and K. Abinaya, "Unified Trust Management Scheme that Enhances the Security in MANET using Uncertain Reasoning," 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2015, pp. 1497-1505.

[16] M. M. Alani, "MANET security: A survey," IEEE International Conference on Control System, Computing and Engineering (ICCSCE), Batu Ferringhi, 2014, pp. 559-564.

[17] S. V. B. Rakas and V. V. Timcenko, "Quality of Service and Security Issues in MANET Environment," 22nd Telecommunications Forum Telfor (TELFOR), Belgrade, 2014, pp. 419-422.

[18] K. T. Selvi and S. Kuppuswami, "Enhancing Security in Optimized Link State Routing protocol for MANET using Threshold Cryptography Technique," International Conference on Recent Trends in Information Technology, Chennai, 2014, pp. 1-6

[19] A. B. C. Douss, R. Abassi and S. G. E. Fatmi, "A Trust Management Based Security Mechanism against Collusion Attacks in a MANET Environment," 9th International Conference on Availability, Reliability and Security, Fribourg, 2014, pp. 325-332.

[20] A. S. Kumar and E. Logashanmugam, "To enhance security scheme for MANET using HMAC," 2nd International Conference on Current Trends in Engineering and Technology (ICCTET), Coimbatore, 2014, pp. 467-471.

[21] G. Kulkarni, B. Patel and P. Laxkar, "Time stamp based Cross Layer MANET Security Protocol," 3rd International Conference on Computational Intelligence and Information Technology (CIIT), Mumbai, 2013, pp. 191-199

[22] A. Echchaachoui, A. Choukri, A. Habbani and M. Elkoutbi, "Asymmetric and Dynamic Encryption for Routing Security in MANETs," International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, 2014, pp. 825-830.

[23] P. Rajakumar, V. T. Prasanna and A. Pitchaikkannu, "Security Attacks and Detection Schemes in MANET," International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2014, pp. 1-6.

[24] K. S. Dhanalakshmi, B. Kannapiran and A. Divya, "Enhancing Manet Security using Hybrid Techniques in Key Generation Mechanism," International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2014, pp. 1-5.