AN EFFICIENT ROUTING PROTOCOL FOR MOBILE AD HOC NETWORK FOR SECURED COMMUNICATION AND MINIMIZED POWER CONSUMPTION

Ms.Shilpa Pagnis, Prof. Ajit Kumar Shrivastava

undefined.shilpapagnis@gmail.com,ajitshrivastava@rediffmail.com
Department of Computer Science & Engineering TRUBA, Bhopal, India

ABSTRACT:

Security and reliable communication is challenging task in mobile Ad Hoc network. Through mobility of network device compromised with attack and loss of data. For the prevention of attack and reliable communication, various authors proposed a method of secured routing protocol such as SAODV and SBRP (secured backup routing protocol). The process of these methods work along with route discovery and route maintains, discovery and route maintained needed more power consumption for that process. The power of devices is decrease during such process and network lifetimes expire. In this paper, we modified the secured stateless protocol for secured routing and minimized the utilization of power during path discovering and establishment. For the authentication of group node used group signature technique and sleep mode threshold concept for power minimization. Our proposed technique is simulated in ns-2 and compare to other routing protocol gives a better performance in comparison to energy consumption and throughput of network.

KEYWORDS:

Adhoc network, secured routing, power, path maintained

1. INTRODUCTION

A Mobile Ad Hoc Network (also called MANET) is a collection of portable devices that establish communication without the help of any infrastructure or established communication backbone [1]. Furthermore, Mobile Ad hoc networks- Do not need backbone infrastructure support, Are easy to deploy, Useful when infrastructure is absent, destroyed or impractical also MANET is used many applications, such as, Military environments, Soldiers, tanks, planes, taxi cab network, Emergency operations, search, rescue, policing etc. Each device in a MANET is free to move independently in any direction, therefore change its links to other devices over and over again. Characteristics of mobile ad-hoc network are self-organizing, multi-hopping, mobility, scalability, security, energy conversation and autonomous devises which makes MANET suitable for up-coming needs also adds complexity to the protocols to be design. The major challenge in building a MANET is

DOI : 10.5121/ijans.2013.3201

equipping each device to continuously maintain the information required to properly route load. Multicasting is a type of delivering messages from one node to set of nodes simultaneously in efficient manner [10]. In the multicasting process the message is transmitted only once (no retransmission) over the network and is duplicated only at the branch point. It reduces the bandwidth consumption in network, which is possible in videoconferencing and distributed gaming like environment, where the same channel is accessed by many users. The protocols used in multicasting can be categorized in two types 1) Source Based Multicasting Protocols (ADMR, MAODV) and 2) Mesh Based Multicasting Protocols (ODMRP, CAMP)[12]. During transmission messages can be stolen and altered or services disruption is also possible in the network; which is called attack. There are many types of attack: 1) Active attack where intention is to alter the information and make the network overload, 2) Passive attack where intention is to steal the message and eavesdrop on the communication, 3) Impression attack which is also known as spoofing where attacker assumes the identity of another node in the network, so that receiving messages directed to the node it fakes, 4) Sinkhole attack where a compromised node tries to attract the data to itself from all neighboring nodes using loopholes in routing algorithms and 5) Wormholes attacks where a malicious node uses a path outside the network to route messages to another compromised node at some other location in the network Transmitter [16]. The rest of paper is organized as follows. In Section II, related work III proposed model. In section IV simulation and result analysis. Results followed by a conclusion in Section V

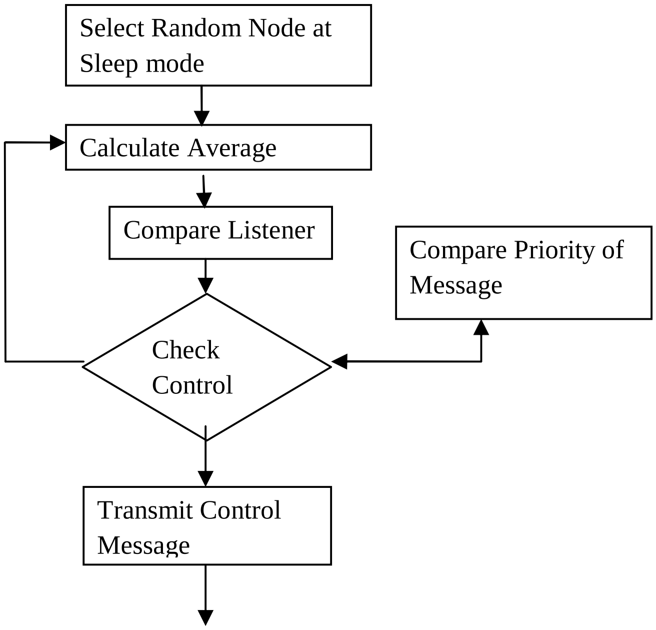
2. RELATED WORK

In this section we discuss related work in the field of malicious attack in adhoc and wireless network in concern of security and power utilization. Patroklosg ,Argyroudis and Donalo Mahony entitled “secure routing for mobile ad hoc networks. The assumption of a trusted environment is not one that can be realistically expected; hence, several efforts have been made toward the design of a secure and robust routing protocol for ad hoc networks. Although the authors mention challenges such as quality of service support and location-aided and power-aware routing approaches, there is no mention of security considerations. Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan entitled “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in manets” 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect is proposed [2]. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Zonghua Zhang, Farid Nait-Abdesselam, Pin-Han Ho and Xiaodong Lin entitled “RADAR: a Reputation-based Scheme for Detecting Anomalous Nodes in Wireless Mesh Networks” a novel anomaly detection scheme, called RADAR, to detect anomalous mesh nodes in wireless mesh network is proposed [3]. RADAR scheme provides features for evaluate each node’s behavior by abstracting and examining appropriate observations using reputation and captures the node’s behavior drifts in terms of reputation by exploring their temporal and spatial properties respectively. Soufine Djahel, Farid Na¨ıt-Abdesselam and Ashfaq Khokhar entitled “An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol” a problem of cooperative black hole attack is proposed [4]. Cooperative black hole attack results in dramatic disruption of the network performance. An acknowledgment based scheme to detect malicious nodes and isolate them from the forwarding process is proposed by the author. Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour,Yoshiaki Nemoto and Nei

Kato entitled “A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks” a new anomaly-detection scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals is proposed [5]. This dynamic learning process calculates the projection distances based on multidimensional statistics using weighted coefficients and a forgetting curve. Zhengming Li, Chunxiao Chigan and Danniel Wong entitled “AWF-NA: A Complete Solution for Tampered Packet Detection in VANETS” a novel scheme called Autonomous Watchdog Formation is proposed [6]. Autonomous Watchdog Formation is enabled by 2-hop Neighborhood Awareness (AWF-NA), to ensure nodes automatically functioning as watchdogs to monitor the behaviors of the relaying nodes.[7] et.at. In packet dropping attack is a node denies to corporate or forwards each other’s packet to save its resources or disrupt the communication. [8]Trust is a degree of belief about behavior of a particular entity. Author suggests various design concepts to develop a MANET trust management system. Suggestions include that trust metric must have unique properties of trust, a trust management design must support cognitive functionality for each node to achieve adaptability to changing network conditions, a trust management system should be situation specific or situation aware, a trust management design must allow optimal settings to be identified under various network and environmental conditions so as to maximize the overall trust of the sys-tem for successful mission executions.

3. MODIFIED SECURED ROUTING PROTOCOL

The secured routing protocol play important role in mobile ad hoc network. Secured routing protocol defended the attack such as worm whole attack, black hole attack and other internal and external attack. In modification of on-demand routing protocol for prevention of attack, various author are proposed a method such as EAODV (Enhanced on demand distance vector routing protocol) and SBRP (secured backup routing protocol).SBRP is very efficient protocol for secured communication in ad hoc network[19]. The process of Secured backup routing protocol executes in three phase. (1) Secured route discovery across the node (2) backup node setup (3) route maintenance across the node. The secured process takes time for execution of process of SBRP protocol. The process of SBRP protocol are not energy efficient, but it is secured protocol against external and internal attack of ad hoc network. The process of activation of SBRP protocol divided into three groups for energy saving mode such one is sleep mode, transit mode and active mode of action of node. For the reduction of power consumption, we modified the activation process of control message protocol according to sleep mode, transit state and active mode. The modified protocol acquired the process of thresholds priority Oder on the basic of neighbor’s node. The selection of neighbor node deepens on the mode operation in three sections. According to order of state create cluster of priority of group. After creation of group calculate average threshold value, compare each group value with minimum threshold value, and pass the control message for communication. Through this process mode of activation, state of node is minimized the time of route establishment and maintenance. The selection of proper node in minimum time and other node in sleep mode the consumption of power is reduces. We modified SBRP protocol for selection of node during on demand request node according to sleep and activation mode of communication. Each node locally assigned priority value of node. . P=$\sum_{I=0}^{M-1} Pi, i+1$ is the power of selected node.The number of nodes in a group called the activation group of node and denoted by GA. Having the same group at all nodes ensures that same average thresholds value. The node neighbors a and b are unaware that they have selected by thresholds value. Having observed a collision in its local time t, node w transmits at time t+GA, creating spurious thresholds with both a and b. the process block diagram is given below.



Protocol steps for modified control message protocol

- Initialized node state
- Initial selection value is set 0
- Calculate the power of energy of selected node for request as
  P=$\sum_{I=0}^{M-1} Pi, i + 1$ here the group of node is M-1 and node selection is 0 to M.
  If Power of node is minimum Pi then selected group of activation
- Create group activation phase
- GAi[t] ← 0,t=0.....GA-1
- ti ← 0 single node in network
- now selection of single node in group node calculate total power of Transceiving power as $P = \sum_{i=0}^{M-1}(pi, i + 1 + Pr)$ for selection of active node for calculating a neighbor threshold as
- Tval=$\sqrt{Pxi - Pyi}$
- If value of Tval is less than selected node power value then selected lower power node as master
- If node=0 then
- Select ← Random(0....gGA-1)
- Send control message
- If not priority group then
- If send any group of priority at transmitter then
- node ← 0
- else if node ++≥1/priority node then
- node ← active mode

4. SIMULATION AND RESULT ANALYSIS:-

For the effectiveness of our proposed model simulate in discrete network simulator ns-2, and used some standard parameter for performance analysis.

Parameter	**Value**
Simulation duration	**100 sec**
Simulation area	**1000*1000**
Number of mobile node	**25**
Traffic type	**Cbr(udp)**
Packet rate	**4 packet/sec**
Abnormal node	**2**
Host pause time	**10sec**

Table 1 shows the simulation parameter of our network

Performance Parameter:-

Throughput: It gives the fraction of the channel capacity used for useful transmission (Data packets correctly delivered to the destination) and is defined as the total number of packets received by the destination. It is in fact a measure of the effectiveness of a routing protocol [14].

Average end-to-end delay: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times[7].

Packet delivery fraction: The ratio of the data packets delivered to the destinations to those generated by the traffic sources [10]

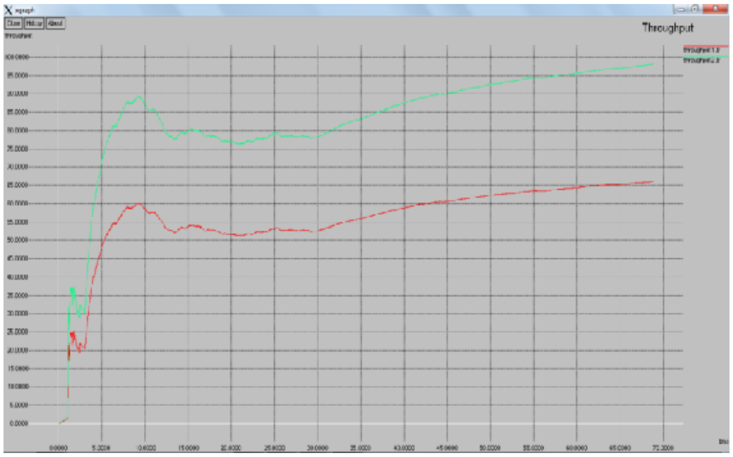


Fig.1 shows that throughput of our network simulation in given scenario for both protocol SBP and modified SBP protocol. Throughput is calculated on the biases of packet delivery ratio to source to destination mobile node.

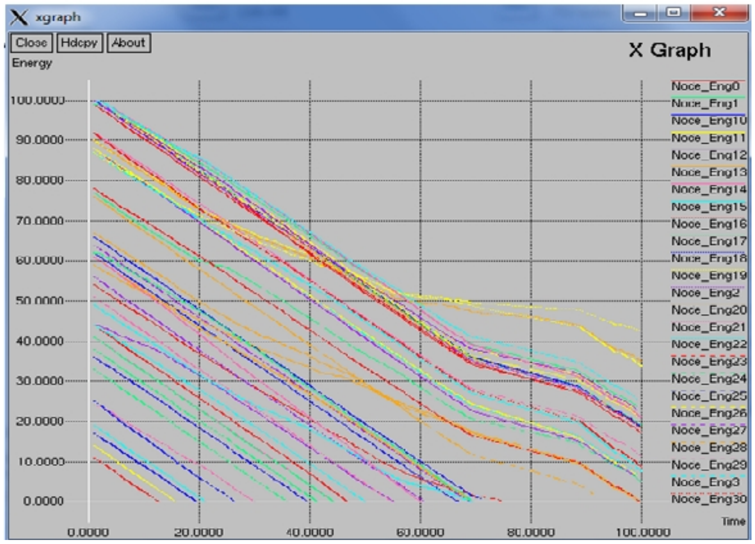


Fig.2 shows that the energy variation in both protocol SBP and Modified SBP routing protocol for given network parameter. The analysis of energy model gives a information about lifetime of network in given time duration. The modified SBP routing protocol increase life time of network.

5. CONCLUSION

In this paper we modified the secured stateless protocol for secured routing and minimized the utilization of power during path discovering and establishment. For the authentication of group node used group signature technique and sleep mode threshold concept for power minimization. The proposed algorithm divide node in two states sleep mode and active mode. The process of going node sleep to active mode calculates priority of all sleep node and compare with arithmetic mean of threshold. The value of sleep mode greater and equal to threshold thus acts as master node in group. In this fashion the utilization of power minimized on time of group communication. Our experimental result shows maximum life time network in comparison to SBRP routing protocol. In future we also improved the key authentication mechanism in group communication.

ACKNOWLEDGEMENT

The author would like to acknowledge Prof.Ajit Shrivastava and Prof.Amit Saxena for their valuable discussions and suggestions.

REFERENCES

[1] Patroklosg. Argyroudis AND Donalo'Mahony "secure routing for mobile ad hoc networks" in IEEE Communication, 2005.

[2] Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" in IEEE Transaction, 2007.

[3] Zonghua Zhang, Farid Nait-Abdesselam, Pin-Han Ho and Xiaodong Lin "RADAR:aReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks" in IEEE Communications Society, 2008.

[4] Soufine Djahel, Farid Na¨ıt-Abdesselam and Ashfaq Khokhar "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol" in IEEE Communications Society, 2008.

[5] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour,Yoshiaki Nemoto and Nei Kato "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" in IEEE Transactions On Vehicular Technology, 2009.

[6] Zhengming Li, Chunxiao Chigan and Danniel Wong "AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs" in IEEE Communications Society, 2008.

[7] Soufiene Djahel, Farid Nait-abdesselam and Zonghua Zhang "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE Communications Surveys, 2011.

[8] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen "A Survey on Trust Management for Mobile Ad Hoc Networks" in IEEE Communications Surveys, 2011.

[9] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture" in IEEE Transaction, 2011.

[10] Ian F. Akyildiz, Xudong Wang and Weilin Wang "Wireless mesh networks: a survey" in Science Direct, 2004.

[11] E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj and B.Prabhu "Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks" in IEEE Transaction, 2011.

[12] Jin Xu "Multicast in Wireless Mesh Networks" in IEEE Transaction.

[13] Capkun S., Buttyan L. and Hubaux J. "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks" in ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), 2003.

[14] Chiu H. S, Lui K. S. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", In International Symposium on Wireless Pervasive Computing.

[15] Djenouri D., Khelladi L. and N. Badache "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks" in IEEE Communication Surveys & Tutorials, 2005.

[16] Hu Y-C., Perrig A. and Johnson D.B "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" in proceedings of ACM Workshop on Wireless Security, 2003.

[17] Hu L., Evans D. "Using Directional Antennas to Prevent Wormhole Attacks" in Proceedings of the 11th Network and Distributed System Security Symposium, 2003.

[18] Khalil I., Bagchi S. and Shroff N.B. "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks" in International Conference on Dependable Systems and Networks, 2005.

[19] G. Lavanya, C.Kumar and A. Rex Macedo Arokiaraj" Secured Back up Routing Protocol for Adhoc Networks" International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010

AUTHORS

Ajit Kumar Shrivastava received the BE degree in computers from University of Pune, in 1997, and the M.Tech degree in computer science & engineering from Rajiv Gandhi Proudhyogiki Vishwavidyalaya in 2007. Pursuing Ph.D. from Mewar University, Chhittaurgarh, Rajasthan, INDIA. He is currently an associate professor in the Department of Computer Science at TRUBA Institute of Engineering and Information Technology, Bhopal (M.P.), INDIA. His recent research activities focus on theoretical issues in GreenIT, Image Processing, channel allocation algorithms in cellular mobile networks.

Shilpa Pagnis received BE degree in Computer Science and Engineering with Honors from RGPV University, Bhopal(M.P) in 2006.Presently pursuing M.tech from RGPV University, Bhopal. Before Joining masters degree in 2008 she did job in VNS Institute of Engineering and Technology for two years as aSenior Lecturer in Department of Computer Science. Her interest is in the field of Adhoc Networks.