INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

SHELTERED ENERGY AWARE ROUTING AGAINST BLACK HOLE ATTACK

Mohammed Abdul Bari*[1], Sanjay Kalkal[2] & ,Shahanawaj Ahamad[3]

[*1]Associate Professor, Dept. of Computer Science &IT Engineering, Nawab Shah AlamCollege of Engineering & Technology, Hydereabad ,Telangana, India

[2]Assistant Professor & Head of Department, Kalinga University, Raipur, Chhattisgarh ,India.

[3]Assistant Professor, Dept. of Computer Sc. & Software Engineering, College of Computer Science & Engineering, University of Ha'il,Kingdom of Saudi Arabia

Keywords: MANET, Black hole, Energy, Algorithm, QoS, Cluster.

Abstract

Mobile ad-hoc network tools are blueprints to set up internet access anywhere and anytime, describes by not having infrastructure, nodes in a system free to portable and categorized themselves in an critic advance, Communication may have additional than one link and diverse radio, can operate in a stand-alone mode. Due to its distinguishing, it needs an proficient dynamic routing protocol in terms of energy as well as refuge due to its characteristic.We propose a "sheltered energy aware routing against black hole attack". It improves the life time of arrangement and shield from black hole attack. It considers the node's power reduction ratio with esteem to current energy & traffic circumstances for -energy awareness, and loose mode for -securing against black hole attack. The results produced by replication have shown that this work is better than existing MBCR and MRPC interns of network lifetime and sheltered interns of black hole attack using NS2.

Introduction

The blueprint aim of MANETs [3] is to hold up internet admittance anywhere any time with awol of infrastructure with self-configured & self-maintenance diagnostic .It is a wireless infrastructure less network composed of collection of motley mobile nodes which are affiliated by a dynamically unstable network topology and absence of central coordinator and network intelligence placeless inside every mobile node so as to nodes in a network act as a router as well as host to form peer to peer network. The connectivity among mobile nodes may have a more than one links and motley radio and can operate in a standalone passion. Due to its diagnostic MANETs well suitable for a circumstances where infrastructure is inconvenient to setup, cost or/and time effective.

The growth, blueprint & execution ambition of MANETs tremendously include in routing, QoS, refuge, multicasting, service discovery, quantifiability & Resource organization such as energy, bandwidth, delay and battery power. The routing procedure design subject is intrinsically related with MANET's applications. Where routing protocols design plan, first and foremost include path discovery from source to destination but in MANETs it must incorporate QoS, resource management with security. Routing protocols is effective when it offers tolerable communication services like route discovery time, communication throughput, end to end delay, and packet loss. QoS routing is the process to furnish end to end loop free path with ensure the necessary parameters of QoS like bandwidth, jitter, delay has to be met. QoS parameter varies with respect to application. Reducing or organizing energy cost during communication is effective factor \ for MANETs routing due to its energy Constraint characteristic, just considering energy consumption during end to end packet travelling is not reliable routing but it also consider reliable links and residual energy of nodes which not only improve QoS but also improve life time of network. Any MANET's submission sheltered statement is vital; primarily in military application security is compulsory. Routing, QoS & protection is demanding in MANETs compared to communications network due to its uniqueness like dynamic network topology, nonexistence of pre-established communications for central management, mobility of nodes, resource control, error prone channels and hidden , depiction node problem. Hence MANETs necessitate of routing protocol which necessity address the MANETs challenges as well as uniqueness. The routing protocol must be completely circulated and adaptive to system dynamics, loop free with route creation and continuation effort must be least amount in time, energy, power and memory. Finally it must bear certain level of QoS parameters with protection. Black hole [14][15] criticize is one of the lively attacks possible in MANETs. On receiving a RREQ message the black hole node, lacking checking for a fresh route, straight away sends false RREP with high series number to the source node. On getting this RREP, the source node create route to this node presumptuous that it has fresh route to purpose and sends its data packets over this route. However, when the packets are sent on this route the black hole node take in the packets without relaying them further. Thus, black hole attack takes place

In this paper we recommend a routing protocol called "secure energy aware routing against black hole attack". This is on top of accessible cluster-head gateway switch routing protocol. The lingering paper organized as follows: Next section portray about Energy efficient routing and secure routing against black hole attack in MANETs. In section 3, Performance evaluation Section 4 discuss related work & our work end with simulation and conclusion

Back Ground

Due to MANETs energy limitation characteristic, consideration of energy cost in routing is an powerful factor so as to reduce the energy during communication. Routing protocol just aim to find the energy aware routing or calculating energy consumption during communication is not reliable routing but also take care of reliable link and node's residual energy which help to improve life time of network and some part of QoS. So far number of routing protocols has been proposed which mainly focus on to improve reliability, energy efficiency and life time of network. e.g., [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13],[14], [15]. These routing protocols are majorly sub divided into three categories

1. Protocols that aim to find more reliable routes through reliability of links.
2. Protocols that aim to find the energy-efficient routes
3. Protocols that aims to finding the routes with higher energy nodes to Improve the life time of network

In MANETs black hole attack is a serious concern which needs a solution, where in black hole attack an attacker intercept the information of MANETs communication. Major security problem arise in MANETs whenever attacker become a part of route, which is created between sources to destination. So far various Routing protocols have been proposed to mitigate black hole attack in MANETs e.g., [21-26] which takes the help of Public Key Infrastructure (PKI) to find secure route , but network has to depend on third party such as PKI, which adds extra overhead regarding key maintenance and distribution. And the protocols [14-20] mainly focus to mitigate black hole attack depending on packet drop without considering the reasons for packet drop.

Cluster

A number of cluster schemes were proposed during the past decade for the secure ad hoc network propagation.The propose of the clustering schemes is to enable better understanding and improvement in secure protocols. This is done by systematic classification. In secure mobile ad hoc networks movement data through the cluster nodes. The rapid changes occur in topology results in overhead data in topology. Protocol maintains cluster nodes in an cluster. Under the pre defined threshold which maintain constant operation of medium control access control protocol.The propose cluster head invoked is to decrease the

1. Identifier-based clustering
2. Connectivity-based clustering
3. Mobility-aware clustering
4. Low cost of maintenance clustering
5. Power-aware clustering
6. Combined-weight based clustering

In this paper we design a routing protocol which aims to improve network life and secure against black hole attack so as to improve the QoS based on residual energy & current traffic of node. In our work we are considering the impact of multiple transmissions over multi hop MANETs on an energy constraint intermediate node. We take consideration of node's energy reduction ratio within an available energy and current traffic; based on it we select a cluster head and make the cluster head in promiscuous mode, which help to monitor the member nodes of cluster. Our contribution of work mainly as follows.

ISSN: 234-5197
Impact Factor: 2.715

1. Calculation of energy reduction ratio of node with respect to current traffic and residual energy of node
2. Selecting Cluster head
3. Detecting and preventing black hole by promiscuous mode

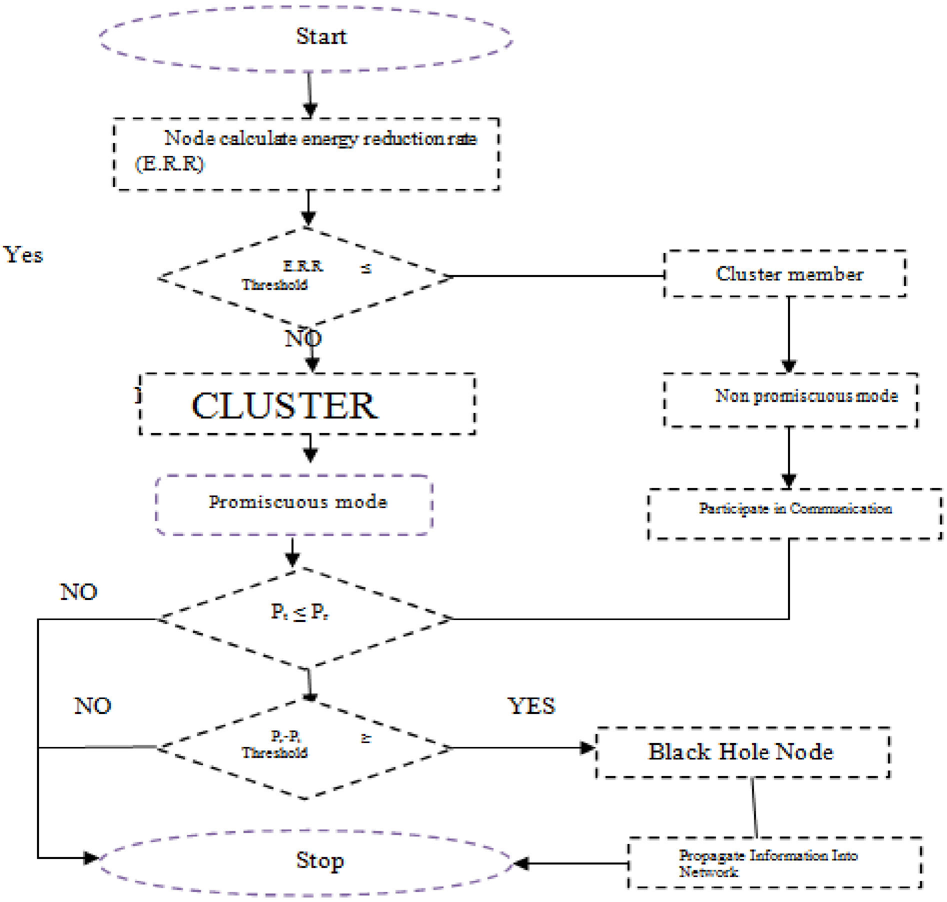
Proposed Model

Our model is based on existing CGSR [26] protocol and improvement on that protocol is selection of cluster head and provide cluster head in a promiscuous mode. Remaining thing is same as in CGSR routing, and named as "secure energy aware routing against black hole attack". [28]This is on top of available cluster-head gateway switch routing protocol. Cluster head selection based on the lower energy reduction rate. This value shows the current situation of node with respect to energy and current traffic. If number of nodes targeting a node as an inter mediate node for their route selection at that situation node become a bottleneck and start to drop the packets, at the same time its energy consumption rate tends to high. In our routing we are tacking the help this value to select the cluster head.

Energy reduction rate is calculated by below formula

$$\frac{\text{currentenergyofnodex}}{\text{energyconsumptionattimet}(\Delta(x))} \ldots\ldots\ldots\ldots\ldots\ (1)$$

Algorithm



In our approach, every cluster head in a network listens to its cluster member nodes promiscuously. In promiscuous mode, cluster head monitors the packet being forwarded by its member neighbors in order to observe the behavior of member nodes regarding packet operation. Cluster head maintain the knowledge table compares the member information with the information it stores in its knowledge table. If both are same the cluster head assumes that the packet is forwarded further, otherwise cluster waits for particular amount of time and checks the reasons for packet dropping. In order to confirm packets communication, the cluster head monitor the control packets as well as data packets to prevent selective dropping, as black hole attack drops selected packets. In order to monitor the forwarded packets, every cluster head has to maintain knowledge tables with following entries: regarding packet forwarding information and member operation on that packet, if both information is differ; the nodes are black hole nodes. If cluster head detects packet not forwarded by cluster members at that instance cluster head checks the other reason for packet not forwarded. If the packet dropping reaches to a threshold value the node is identified as malicious node and is removed from route selection. And broadcast the information to its all other members so as to remove that node to using for communication.

Performance Evaluation

We investigate the performance of proposed RER-SK model using the ns-2 simulator with the necessary extension and compare it with MBCR [8] &MRPC [27] in a same condition with respect to network life time and compare with AODV with respect to packet delivery ratio interms of number of malicious nodes. In our simulations, we use a fixed transmission range of 250 meters, which is supported by most of real time and current network interface cards. We used the “random waypoint” with speed of nodes is uniformly distributed between 0 to maximum speed of 20 m/s with pause time value of 40 sec. All mobile nodes to be equipped with IEEE 802.11 network interface card and data rates of 3 Mbps. The initial energy of all the nodes is 15J. The transmission power is 650mW and the receiving power is 350mW. Finally, source nodes generate CBR (constant bit rate) traffic. Traffic sessions are generated randomly on selected different source- destinations with a packet size of 512 bytes. Every node in a network has to run our algorithm whenever it becomes an intermediate node to forward the information of source nodes. Each simulation was run for the duration of 300 seconds and sampled data we collected from simulation is average of 3 times.

Our aim is mainly calculate energy reduction ration of each node in a network with respect to current battery as well as traffic condition,and according to it select the cluster head. We therefore measure the network lifetime, reliability of link with respect to packet delivery ratio and compare it to existing MBCR [8], MRPC [27].The network life time in our work is considered as a time that the first node failure occurs in a network due to exhausting of battery. Delay in the failure of first node impacts on other node to be delayed. Fig.1 shows the performance of Proposed approach, MBCR & MRPC as function of the packet delivery ratio with respect to network life time. This fig1 clearly shows proposed approach can significantly delay the first node failure compare to other algorithms...In fig2 shows the finding energy efficient route compare to other, where less amount of energy consumed to route a packet. In conclusion, Proposed approach increases the lifetime of network .for Fig 3, Black hole nodes have been created and analyzed the result of simulation with the above specified scenario and compare it with existing MCBR, MRPC., and calculate the packet delivery ratio.

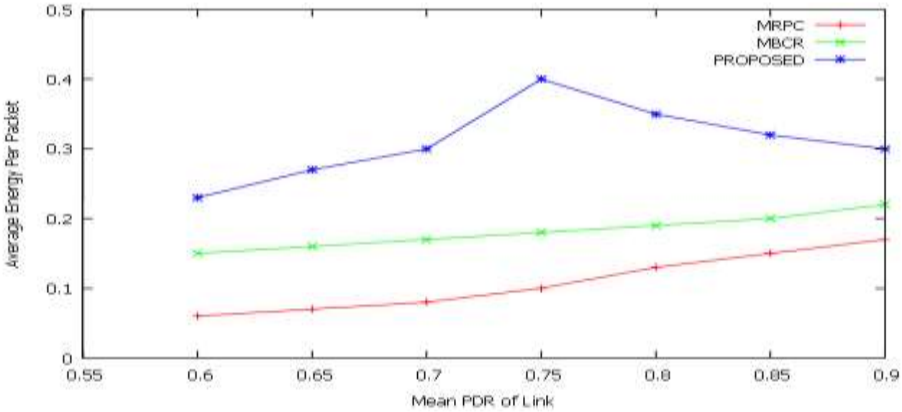


Fig.1.AverageNumber of packetsdelivered to destination with respect tonodefailure in a network

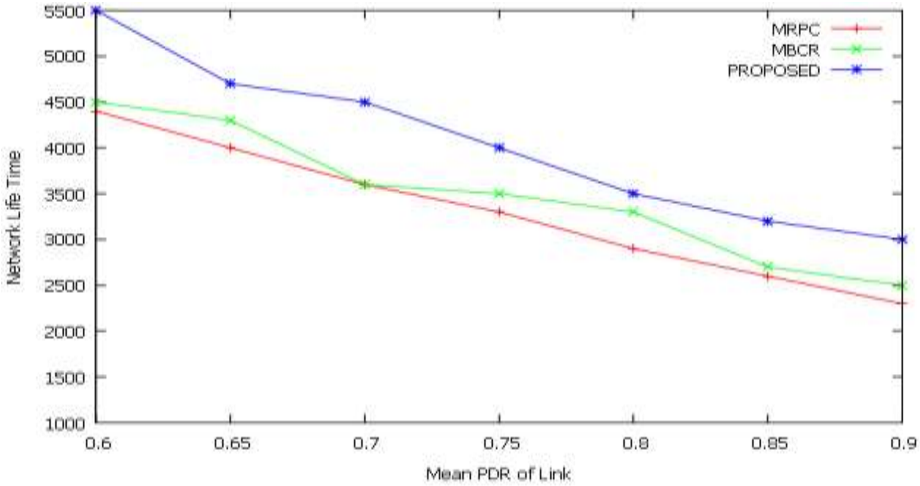


Fig.2.AverageEnergy consumed toroute packet fromSourceto Destination

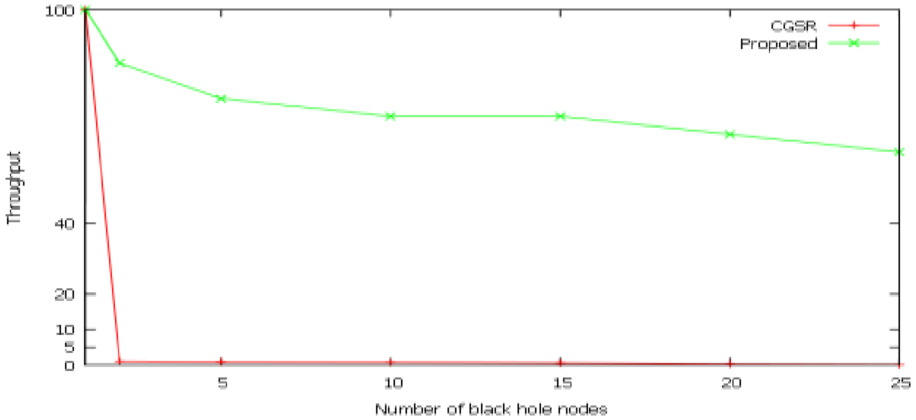


Fig.3. Packet delivery ratio vs number of malicious node with 100sec Simulation time

Conclusion

In this attempt we projected a new Protocol, "secure energy aware routing against black hole attack" which is used to maintain the life time of network as well keep beside black hole attack. The metric energy reduction ratio of node settle on, whether node to be develop into cluster head or not. And with the help of monitoring we are avoiding black hole attack.. The foremost goal of planned approachis not only makes best use of the network life time but also securing with black hole attack.

References

1. S X.-Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, "Reliable and Energy-Efficient Routing for Static Wireless Ad Hoc Net-works with Unreliable Links," IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 10, pp. 1408-1421, Oct. 2009.
2. A.B. Mohanoor, S. Radhakrishnan, and V. Sarangan, "Online Energy Aware Routing in Wireless Networks," Ad Hoc Networks, vol. 7, no. 5, pp. 918-931, July 2009
3. D.J Vergados, N.A. Pantazis, and D.D. Vergados, "Energy-Efficient Route Selection Strategies for Wireless Sensor Net-works," Mobile Networks and Applications, vol. 13, nos. 3-4, pp. 285-296, Aug. 2008.
4. A. Nagy, A. El-Kadi, and M. Mikhail, "Swarm Congestion and Power Aware Routing Protocol for Manets," Proc. Sixth Ann. Comm. Networks and Services Research Conf., May 2008
5. X. Li, H. Chen, Y. Shu, X. Chu, and Y.-W. Wu, "Energy Efficient Routing with Unreliable Links in Wireless Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '06), pp. 160-169, 2006

6. X.-Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, “Reliable and Energy-Efficient Routing for Static Wireless Ad Hoc Net-works with Unreliable Links,” IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 10, pp. 1408-1421, Oct. 2009.
7. J.-H. Chang and L. Tassiulas, “Maximum Lifetime Routing in Wireless Sensor Networks,” IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.
8. D Kim, J.J.G. Luna Aceves, K. Obraczka, J. Carlos Cano, and P. Manzoni, “Routing Mechanisms for Mobile Ad Hoc Networks Based on the Energy Drain Rate,” IEEE Trans. Mobile Computing, vol. 2, no. 2, pp. 161-173, Apr.-June 2003.
9. J. Gomez, A.T. Campbell, M. Naghshineh, and C. Bisdikian, “PARO: Supporting Dynamic Power Controlled Routing in Wireless Ad Hoc Networks,” Wireless Networks, vol. 9, no. 5, pp. 443-460, 2003.
10. D.S.J. De Couto, D. Aguayo, J. Bicket, and R. Morris, “A High-Throughput Path Metric for Multi-Hop Wireless Routing,” Proc. ACM MobiCom, pp. 134-146, 2003.
11. A. Misra and S. Banerjee, “MRPC: Maximizing Network Lifetime for Reliable Routing in Wireless Environments,” Proc. IEEE Wireless Comm. and Networking Conf. (WCNC ’02), pp. 800-806, 2002.
12. S. Banerjee and A. Misra, “Minimum Energy Paths for Reliable Communication in Multi-Hop Wireless Networks,” Proc. ACM MobiHoc, pp. 146-156, June 2002
13. S. Singh and C. Raghavendra, “PAMAS—Power Aware Multi-Access Protocol with Signalling for Ad Hoc Networks,” ACM Computer Comm. Rev., vol. 28, pp. 5-26, 1999.
14. Fidel Thachil, K.C. Shet, "A Trust Based Approach for AODV protocol to Mitigate Black hole attack in MANET ," 2012 International conference in Computing Science.,IEEE 2012.
15. DurgeshKshirsagar, AshwiniPatil, “Blackhole Attack Detection and Prevention by Real Time Monitoring”, 4th ICCCNT 2013, July 4-6, 2013, Tiruchengode, India.
16. TamilSelvan, L.; Sankaranarayanan, V., "Prevention of Black hole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on , vol., no., pp.21,21, 27-30 Aug. 2007.
17. Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method.” In: International Journal of Network Security, Vol. 5, No.3, pp.338–346, Nov. 2007.
18. Sukla Banerjee, “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, World Congress on Engineering and Computer Science , October 2008, pp. 337-342.
19. Payal N. Raj, Prashant B. Swadas. “DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet.” In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009.
20. Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit, “A Novel Approach for Detection ofBlackhole Attacks” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 69-74
21. A.Rajaram, Dr. S. Palaniswami,”Malicious Node Detection System for Mobile Ad hoc Networks”, International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010.
22. Y.-C. Hu, D. B. Johnson, and A. Perrig, “Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks,” The 4th IEEE Wksp. Mobile Computing Systems and Applications (WMCSA’02), June 2002.
23. Y.-C. Hu, D. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Ad Hoc Networks, Elsvier, vol. 1, no. 1, 2003.
24. C. Castelluccia and G. Montenegro, “Protecting AODV Against Impersonation Attacks,” ACM SIGMOBILE Mobile Comp. and Commun. Rev. Archive, vol. 6, no. 3, July 2002.
25. P. Papadimitratos and Z.J. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS’02), Jan. 2002.
26. C.C Chiang at all”Routing in cluster Multi hop ad hoc networks with fading channel ”proceeding of IEEE SICON 1997 pp197-211
27. Kuei-Ping Shih, Chau-ChiehChang ,Yen-Da Chen, “MRPC: A Multi-Rate Supported Power Control MAC Protocol for Wireless Ad Hoc Networks ” Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE
28. M.A.Bari,Sanjay Kalkal,Shahanawaj Ahamad," A Comparative Study and Performance Analysis of Routing Algorithms for Manet",ICCIDM 2016,Springer.