Volume 2, Issue 1, January 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Consequences of limited manet resources

Pooja Malik
Department of Computer Science and Engineering,
Indo Global College Of Engineering, Punjab Technical University,
Kapurthala (Punjab), India.

Abstract— **This paper discusses the ad-hoc network basically the MANET(Mobile Ad-hoc network),types of MANET, its characteristics, application performance issues , resources requirements of manet, consequences of limited resources.**

Keywords— **Ad-Hoc , MANET, selfish nodes, DOS, malicious nodes**

I. INTRODUCTION

Ad hoc networks are a key factor in the evolution of wireless communications. Self organized ad hoc networks of PDAs or laptops are used in disaster relief, conference, and battlefield environments. These networks inherit the traditional problems of wireless and mobile communications, such as bandwidth optimization, power control, and transmission-quality enhancement. In addition, their multihop nature and the possible lack of a fixed infrastructure introduce new research problems such as network configuration, device discovery, and topology maintenance, as well as ad hoc addressing and self-routing.

II. MANET

An A "Mobile ad hoc network" is a system of wireless mobile nodes with routing capabilities –the union of which form an arbitrary graph. Any group of them are capable of forming an autonomous network that require no infrastructure and is capable of organizing itself into arbitrary changeable topologies. Such a network may operate in a stand alone fashion, or may be connected to the larger Internet . The definition, which is given by the Internet Engineering Task Force (IETF).Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc. Unlike traditional mobile wireless networks, Ad hoc networks d on't rely on any fixed infrastructure(base stations, access points).
This flexibility makes them attractive technology for many applications such as rescue and tactical operations, disaste r recovery operations and educational applications where we can setup virtual class or conferences.

A. Manet types

Vehicular Ad Hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment.

Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

Internet Based Mobile Ad hoc Networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly.

B. Manet charterstics

Autonomous terminal: In MANET, each mobile host is autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

Distributed operation: Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

Multi-hop routing: Basic types of ad hoc routing algorithms can be single-hop and multi-hop. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

Dynamic network topology: Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network.

Fluctuating link capacity: The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous. One effect of the relatively low to moderate capacities is that congestion is typically the norm rather than the exception i.e. aggregateapplication demand will likely approach or exceed network capacity frequently.

Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other means for their energy. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

Limited physical security: MANETs are generally more prone to physical security threats than are fixed cable networks. The increased possibility of eavesdropping, spoofing and denial-of-service attacks should be carefully considered.

C. Manet applications

Military-Ad hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarters .consider a scenario is deployed over a battlefield . The ad hoc network formed by the air vehicle in the sky can provide a backbone for land based platforms to communicate when they are out of direct range,or when obstacles prevent direct communication. The ad hoc network therefore extends down to the land based forces and allows communication across the battlefield. Voice and video, as well as sensing and data applications can be supported.

Disaster Relief - In cases of disasters, the existing infrastructure is often damaged or destroyed.. Natural disasters e.g. lead to the loss of electricity and Internet connectivity, Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. An ad hoc network can be used used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake,, to overcome the problems incurred by missing infrastructure, helping to better cope with the consequences of such calamities. Mobile units carry networking equipment to support routing operations.Information is relayed from one rescue team member to another over a small handheld. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement etc.

III. CONSEQUENCES OF LIMITED RESOURCES

A. Selfish Nodes:

Distributed co-operation among users is a vital factor for the success of any ad – hoc networks. Any presences of selfish node can greatly degrade the performance. A selfish node preserves its own resources while uses the services of others and consumes their resources. Mobile ad hoc networks (MANETs) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and last but not least energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

B. Denial of service: In this attack malicious node floods irrelevant data to consume network bandwidth or to consume the resources (e.g. power, storage capacity or computation resource) of a particular node. Withfixed infrastructure networks, we can control denial of service attack by using "Round Robin Scheduling", but withmobile adhoc networks, this approach has to be exte nded to adapt to thelack of infrastructure, which requires the identification ofneighbor nodes by using cryptographic tool s,and cost is very high.

For example,Assume a shortest path exists from X to Z and R and Z cannot hear each other, that nodes Q and R cannot hear each other, and that Y is a malicious node attempting a denial of service attack. Suppose X wishes to communicate with Z and that X has an unexpired route to Z in its route cache. Transmits a data packet toward Z with the source route X –> P –> Q –> Y –> R –> S –> Z contained in the packet's header.

When Y receives the packet, it can alter the source route in the packet's header, such as deleting S from the source route. Consequently, when R receives the altered packet, it attempts to forward the packet to Z. Since Z cannot hear R, the transmission is unsuccessful.

C. Malicious nodes

The malicious nodes can readily function without *proper* security, as routers and prevent the network from delivering the packets properly. For example, the malicious nodes can declare incorrect routing updates. Subsequently they are propagated in the network or drop all the packets passing through them. Thus security issue in ad hoc networks, specifically the protection of their network-layer operations from malicious attacks, is extremely important. Different types of misbehavior out of different purposes have been created by the misbehavingnodes in an ad hoc network. The types of misbehavior on data related to the work are as follows.

Data Dropping: This is the denial of service (DoS) attack. In this attack, the selfish or malicious intermediate nodes decline to forward data packets for other nodes in the network.They represent the types of data dropping misbehavior formed by individual and cooperating misbehaving nodes respectively.

Data Modifying: During their transmission, the malicious nodes alter the received data packets. One malicious node is assumed to form the data modifying misbehavior independently along the data transmission path.

IV. CONCLUSIONS

A research work has being entirely on the assumptions that certain noeds due to resource constraints like low battery power or limited bandwidth start Misbehaving in network. Due to this a cascading effect may happen where large number of nodes within the network might also not perform work .we suggest a watchdog (monitoring body) approach in monitoring such scenarios there can be one or more nodes which has an in-built mechanism to identify selfish nodes in a network or sub network.

REFERENCES

[1] Tarag Fahad Robert Askwith "*A Node Misbehaviour Detection Mechanism for Mobile Adhoc Networks*" The 7th Annual PostGraduate Symposium on The Convergence ofTelecommunications, Networking and Broadcasting, 26-27 June 2006.

[2] Panagiotis Papadimitratos,and Zygmunt J. Haas *"Secure Data Communication in Mobile Ad Hoc Networks"* Ieee Journal On Selected Areas In Communications, Vol. 24, No.2, February 2006.

[3] Ernesto Jimenez Caballero *"Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem"* 2006.

[4] Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang, "*A secure incentive protocol for mobile ad hoc networks", Wireless Networks (WINET),* vol 13, issue 5, October 2007.

[5] Liu, Kejun Deng, Jing Varshney, Pramod K.Balakrishnan, Kashyap *"An Acknowledgmentbased Approach for the Detection of Routing Misbehavior in MANETs"* Mobile Computing, IEEE Transactions on May 2007.

[6] Li Zhao and Jose G. Delgado-Frias *"MARS:Misbehavior Detection in Ad Hoc Networks"* Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE Publication Date: 26-30 Nov. 2007.

[7] C. E. Perkins, *"Ad hoc On-Demand Distance Vector (AODV) Routing,"* RFC 3561, IETF NetworkWorking Group, 1998.

[8] F. Kargl, A. Klenk, S. Schlott, and M. Weber, 2005, *"Advanced Detection of Selfish or Malicious Nodes in Ad hoc Network"s,* Springer Berlin / Heidelberg.

[9] Levente Buttyan and Jean-Pierre Hubaux, *Stimulating Cooperation in Self-organizing Mobile Ad Hoc*, Technical Report No. DSC/2001/046, Swiss Federal Institute of Technology, Lausanne, July 2001

[10] Jean-Pierre Hubaux, Levente Buttyan, et, al, *Toward Mobile Ad-hoc Wans: Terminodes*, In Technical Report No. DSC/2000/006, Swiss Federal Institute of Technology, Lausanne, July 2000

[11] E. Fratkin, V. Vijayaraghavan, Y. Liu, D. Gutierrez, TM Li, and M. Baker. *Participation Incentives for Ad Hoc Networks*, http://www.stanford.edu/ yl314/ape/ paper.ps

[12] Pietro Michiardi and Refik Molva, *Prevention of Denial of Service Attacks and Selfishness in Mobile Ad Hoc Networks*, Research Report RR-02-063 - January 2002

[13] S. Buchegger, J.Y. Le-Boudec, *Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc networks*, In Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Spain, January 2002

[14] S. Buchegger, J.Y. Le-Boudec, *Performance Analysis of the Confidant Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks)*,In Proceedings of IEEE/ACM Workshop on Mobile Ad HocNetworking and Computing (MobiHOC), Lausanne, Switzerland, June2002

[15] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, *Self-securing Ad Hoc Wireless Networks*, 7th IEEE Symposium on Computers and Communications (ISCC'02), Italy, July 2002

[16] Luzi Anderegg, Stephan Eidenbenz, *Ad hoc-VCG:A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks With Selfish Agents*, In Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom'03), San Diego, September 2003

[17] S. Marti, T. J. Giuli, K. Lai and M. Baker, *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*, In Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom), Boston, August 2000

[18] David. B. Johnson and David A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, In Internet draft, Mobile Ad Hoc network (MANET) Working Group, IETF, October 1999