International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(3), pp.299-302
DOI: http://dx.doi.org/10.21172/1.93.50
e-ISSN:2278-621X

REVIEW OF SECURITY, CHALLENGES AND PROBLEMS IN MOBILE AD-HOC NETWORKS

Dheer Dhwaj Barak[1]

Abstract-MANET is a collection of self -governing nodes, which communicate with each other to supply information unrelated to own Interest. MANET is Infrastructure less network and wireless links. In this paper we studied application, characteristics and challenges of MANETs

1. INTRODUCTION

MANET is an ad hoc network to which a set of free nodes attached. These nodes are capable of altering its locations and topology without requiring any predefined structure. MANET is organized in a central way. Here nodes itself acts as router as well as participating nodes. MANET node depends on acting topology so it facilitates mobility which causes faster speed of a network. But this randomly changing topology has become a challenge for worldwide researchers. This problem has arrived because nodes can act as both participating and router nodes. The main challenge faced while implementation of MANET is due to restricted bandwidth and high battery requirement, availability of which cannot be guaranteed on the go. [Alvarez, 2016] [Sahadevaiah, 2011] [Zhou, 1999]

2. CHALLENGES AND CHARACTERISTICS

It is not an easy task to implement MANET. A lot of challenges are faced while carrying out its execution, which is figured below:

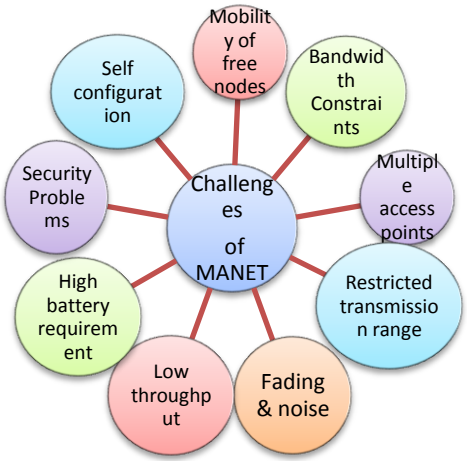

Figure 1: Challenges of MANET

Challenges in MANETs mainly arise due to aspects given below:

- The nodes can freely and randomly move at any time/mobility.
- Low bandwidth / bandwidth constraints /variable capacity links
- Multiple accesses and restricted wireless transmission ranges
- Fading and noise
- Interference conditions and low throughput
- Constrained power/battery/energy constrained operation
- Restricted physical security and modest resources
- Heterogeneous and localized control
- Auto-configuration and dynamic structure
- Lack of unceasing connections

[1] Resource person in CSE Deptt., UIET, MDU, Rohtak

- Security Problems (Refusal of Services Attacks, Indiscretion, Node Concordat, Selfishness, unavailability of information about Network Application / Service – Location and Content, Network Origin, Range, Capability etc.)

Security, attacks, routing protocol and energy consumption are major issues in wireless adhoc networks. The inherent individualities as well as encounters creates a set of original suppositions as well as performance apprehensions for protocol designers which extended outside guidelines of the design of routing which encompass finally higher-speed and semi-static topology of a fixed network [Desilva, 2005] [Kaur, 2014] [Menaka, 2013].

3. PROBLEMS IN MANETS

If preventive measures are not taken at earlier stages of a network, then network operations and various other functions of it can be easily imperilled. As a result MANET nodes may not execute unfavourable network functions properly. Malicious nodes can introduce malicious info into routing packets thereby causing stale loop time-out as well as advertisement of deceitful/ accumulated metrics etc. Some the adhoc protocols are based on a benign environment and these protocols may suffer from security attacks in an adverse environment [Ghaffari, 2006] [Nadeem, 2013] [Hu, 2002] [Specht, 2004] [Sahadevaiah, 2011].

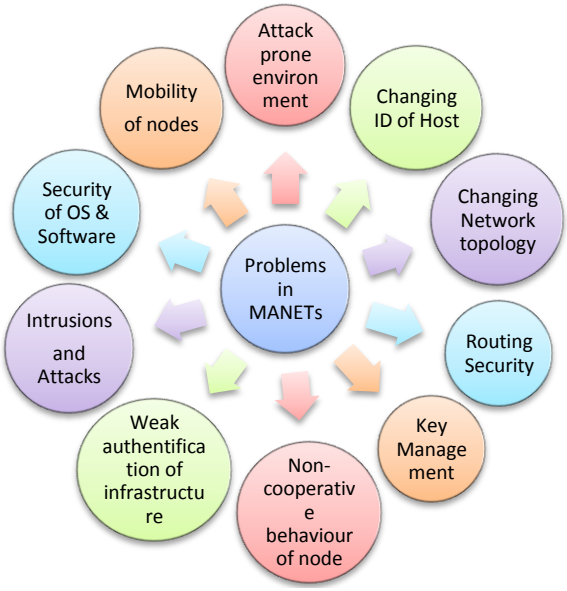

Figure 2: Problems in MANET

Security problems for adhoc networks over other networks were concluded as:

- Attack Prone Environment/Unfriendly Environment
- Node Tracing / Unique Identify a Host / Changing ID of Host
- No Temper Proof Network/Network Topology Changes
- Routing Security / Packet Forwarding and Routing
- Key Management
- Trust Relationship / Selfish behaviour of nodes and Non-Cooperation
- Weak Authentication Infrastructure
- Intrusions and Attacks and Scalable Security
- Operating System / Software / Program / Code Security
- Inter-Vehicle / Moving Nodes / Mobility.

4. SECURITY CHALLENGES AND VULNERABILITY

Traditional wired networks are quite less insecure than which of Mobile adhoc networks It is quite difficult to safeguard the Mobile adhoc networks from the invaders than which of wired network [Nait-Abdesselam, 2008] [Vij, 2016] [Alvarez, 2016].

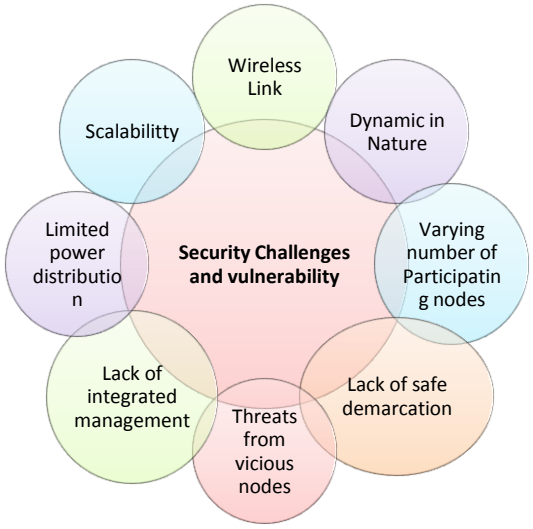

Figure 3: Security challenges and vulnerability

Various security challenges and vulnerabilities which mobile adhoc networks face are as follow:

- Wireless Link: Use of wireless links has posed one of the major problems faced by adhoc networks. Due to the inherent features, an adhoc network is more susceptible to link attacks like passive eavesdropping, active impersonation, message replay and message corruption etc. In "Eavesdropping" a malicious node can garner accessibility even to top-secret info thereby violating confidentiality. "Active attacks" may permit deleting or injecting erroneous messages, modify messages and impersonate as another node in network traffic by a malicious node, thereby violating the features like "availability, integrity, authentication and non-repudiation".
- Dynamic in Nature: Dynamic nature of an adhoc network is mainly responsible for change in discretional nature of its configuration and membership. This nature does not allow the linked nodes to sustain long-term-peer relations among themselves.
- Varying Number of participating Nodes: One must not consider which the participating nodes in an adhoc network can be up to a specific number only. Theoretically, it is possible to form an adhoc network using hundreds or even more number of nodes, though it is not yet implemented practically. So, it becomes necessary to build a security system in such a way which it is capable of managing discretionally large networks and carrying out the tasks assigned to it.
- Lack of Safe Demarcation: Unlike traditional wired network, which gives clearly a secure demarcation line, there is no such line of defense present in mobile adhoc network. Main reason behind this vulnerability of the mobile adhoc network is due to liberty of the nodes to link, detach or move in a network.
- Threats from Peril nodes In a Network: Some intruders target to get the authority over nodes using unfair means, further using malicious nodes for disrupting normal functionality of the network. Malicious node is benefitted due to mobility of adhoc networks which gives it chance to change its target to attack the system frequently, causing intense damage to the whole network system.
- Lack of Integrated Managing Facility: Mobile adhoc networks do not have any integrated management system like a name server, which can cause severe security problems. To perform a particular network operation, it is mandatory for all the nodes to act in a collaborative way, while it is not possible to provide a secure bound to all the network nodes. As it is quite difficult to supervise the data traffic in an ever changing and large adhoc network, so due to unavailability of integrated security management machinery it becomes quite difficult to find out the intruders and their attacks.
- Limited Power Distribution: In case of wired network, nodes are directly connected to the outlets of electric power supply, so they can consume as much power as they require, while in case of mobile adhoc networks, due to dynamic nature of nodes, nodes need to work on a limited power supply. Due to this, a node can act in a selfish way to conserve the power available or can even lead to refusal for the service attacks.
- Scalability: When a customary wired network is premeditated then its scale is usually pre-defined which is not changed much during the usage. On the contrary, scale of adhoc network keeps altering all the time primarily owing to mobility of the nodes. As a consequence, protocols as well as services having applicability in an adhoc network like "routing protocol and key management service" should be well-suited to constantly varying scale of an adhoc network.

Thus, one can conclude which mobile adhoc network is insecure by its nature and require stronger security system to assure network safety as compared to the wired network [Bajaj,1999].

5. CONCLUSION

MANET is one of the fastest emerging network techniques but it has its own pros and cons. Though MANET gives easy multiple accesses but due to this security becomes one of the main problems faced in implementing MANET. Some mechanisms can be developed to enhance network security and this can facilitate its more applications worldwide.

6. REFERENCES

[1] Alvarez (2016), Flor, Matthias Hollick, Paul Gardner-Stephen, "Maintaining both availability and integrity of communications: Challenges and guidelines for data security and privacy during disasters and crises," Global Humanitarian Technology Conference (GHTC), pp 62-70.

[2] Bajaj (1999), L, Takai, M, Ahuja, R, Tang, K, Bagrodia, R, and Gerla, M, "Glomosim: A scalable network simulation environment," Technical report, 990027, UCLA Computer Science Department, pp 1-213. Available on: citeseer.ist.psu.edu/225197.html.

[3] Desilva (2005), S, R.V. Boppana, "Mitigating Malicious Control Packet Floods in Ad HocNetworks," In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC05), pp 2112-2117.

[4] Ghaffari (2006), Ali, "Vulnerability and security of mobile ad hoc networks," In Proceedings of the 6th WSEAS international conference on simulation, modelling and optimization, pp 124-129.

[5] Hu (2002), Yih-Chun, Adrian Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom), pp 12-23.

[6] Kaur (2014), Amandeep, and Amardeep Singh, "A Review on Security Attacks in Mobile Ad-hoc Networks," International Journal of Science and Research (IJSR), vol. 3, no. 5, pp 1295-1299.

[7] Menaka (2013), R, and Dr V. Ranganathan, "A Survey of Trust related Routing Protocols for Mobile Ad Hoc Networks," International Journal of Emerging Technology and Advanced Engineering , vol.3, no. 4, pp 903-910.

[8] Nadeem (2013), Adnan, and Michael Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system," Telecommunication Systems, pp 1-12.

[9] Nait-Abdesselam (2008), Farid, Brahim Bensaou, and Tarik Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," IEEE Communications Magazine, vol. 46, no. 4, pp 127-133.

[10] Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, YudhvirSingh,"Attack Prevention Methods for DDoS Attacks in MANETs", Asian Journal Of Computer Science And Information Technology, ISSN – 2249-5126,Vol 1, Issue 1, pp. 18 – 21 (2011).

[11] ParveenKumari, Yudhvir Singh, "Delaunay Triangulation Coverage Strategy for Wireless Sensor Networks", Proc. of IEEE sponsored Second International Conference on Computer Communication and Informatics (2012).

[12] Pooja, Manisha, Yudhvir Singh, "Security Issues and Sybil Attack inWireless Sensor Networks", International Journal of P2P Network Trends and Technology,ISSN: 2249-2615, Volume3, Issue1, pp7-13, 2013.

[13] Preeti, Yogesh Chaba, Yudhvir Singh, "Review of Detection and Prevention of DDOS attack in MANET", Proc. National Conference on Challenges &Opportunities in Information Technology(COIT –2008), India, pp. 56-59 (March 29,2008).

[14] Prabha Rani, Yogesh Chaba, Yudhvir Singh, "Hybrid Approach for Detection and Prevention of Blackhole Attack in Mobile Adhoc Network",International Journal of Wireless Communication, ISSN 0974-9640, pp 885-890, August, 2011.

[15] Rahul Rishi, Dheer Dhwaj Barak, Yudhvir Singh, Prabha Rani, "Mobility Analysis of Blackhole Node Attacks in Mobile Adhoc Networks", International Conference on"Recent Trends in Computing, Mechatronics and Communication, India,pp 93-97, February 25-26, 2012.

[16] RenuDalal, Manju Khari, Yudhvir Singh, "Survey of Trust Schemes on Ad-hoc Network", Springer - Lecture Notes of the Institute for Computer Sciences, Social Informatics & Telecommunications Engineering (LNICST) Series 84, Springer, NETCOM-3, CCSIT-2012,pp 170-180,(2012).

[17] Sahadevaiah (2011), Kuncha, and Prasad Reddy PVGD, "Impact of security attacks on a new security protocol for mobile ad hoc networks," Network Protocols and Algorithms, vol. 3, no. 4, pp 122-140.

[18] Specht (2004), Stephen M, and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures," In ISCA PDCS, pp 543-550.

[19] Vij (2016), Akansha, Vishnu Sharma, "Security issues in mobile adhoc network: A survey paper," In Proceedings of IEEE International Conference on Computing, Communication and Automation (ICCCA), pp 561-566.

[20] VikashSiwach,Yudhvir Singh, Seema,DheerDhwaj Barak, "An approach to optimize QoS routing protocol using genetic algorithm in MANET", IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 149-53, (Sept 2012).

[21] Yogesh Chaba, Yudhvir Singh, Prabha Rani, "Comparison of Various Passive Distributed Denial of Service Attack in Mobile Adhoc Networks" Proc. WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communication(EHAC 10),Cambridge,UK (ISBN: 978-960-474-155-7), pp 49-53(2010)

[22] Yogesh Chaba, Yudhvir Singh, KP Singh, Prabha Rani, "Performance Modeling of MANET Routing Protocols with Multiple Mode Wormhole Attacks", Communications in Computer and Information Sciences, Springer [Online : Springer Digital Library] (2010) Volume 101, Part 3, pp 518-527, (2010).

[23] Yogesh Chaba, Yudhvir Singh, Aarti, "Performance Analysis of Scalability and Mobility on Routing Protocols in MANETs" International Journal of IT & Knowledge Management (ISSN: 0973-4414) Vol. 1, No. 2, pp. 327-336 (July-Dec, 2008).

[24] Yudhvir Singh, AvniKhatkar, Prabha Rani, Deepika, DheerDhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks" Third IEEE International Conference on Advanced Computing & Communication Technologies, 2012.

[25] Yudhvir Singh, Yogesh Chaba, Prabha Rani, "Integrating – VPN and IDS – An approach to Networks Security", International Journal of Computer Science & Security(ISSN: 1985-1533), Vol. 1, Issue 3, pp. 1-13(2007)

[26] Yudhvir Singh, Amit Kumar, Prabha Rani, and Sunil Kumar Kaushik, "Impact of CBR Traffic on Routing Protocols in MANETs", IEEE UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, [Online: IEEE Xplore Digital Library], University of Cambridge, United Kingdom, 26-28, March 2014.

[27] Yudhvir Singh, DheerDhwaj Barak, VikashSiwach,Prabha Rani,"Attacks on wireless sensor networks: a survey", IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 143-148, (Sept 2012).

[28] Zhou (1999), Lidong, and Zygmunt J. Haas, "Securing ad hoc networks," IEEE network, vol. 13, no. 6, pp 24-30.