ISBN: 978-93-83758-09-8

# Performance Analysis of Mobile Ad-Hoc Network Protocols

Shakti Arora
Head of Computer Science Department
Geeta Engineering College, Naultha (Panipat)
shakti.nagpal@gmail.com

*Abstract:* - **Mobile ad hoc networks are an emerging and popular technology to the world; however, the benefits of them are actually their fragility either. In scenarios of military operations and catastrophes even when there is no infrastructure available or left there is a need for communication. Due to the specific context the communication systems used in these tactical scenarios need to be as reliable as possible. Thus, the performance of these systems has to be evaluated. In mobile ad-hoc networks, nodes do not rely on any routing infrastructure but relay packets for each other. Thus communication in mobile ad-hoc networks functions properly only if the participating nodes cooperate in routing and forwarding.**
**However, it may be advantageous for individual nodes not to cooperate, for example to save power or to launch security attacks such as denial-of-service. In this paper, we give an overview of potential vulnerabilities and requirements of mobile ad-hoc networks, and of proposed prevention, detection and reaction mechanisms to thwart attacks.**

*Keywords:*- **Performance analysis, Mobile Networks, Routing Protocol,**

## I. INTRODUCTION

The goal of this paper is to study whether the advantages of cooperative (peer-to-peer) content distribution as seen in the Internet can carry over in ad hoc networks. To do this, we develop an application layer content distribution scheme and we study its performance extensively.

As the communication systems used in these tactical or disaster area scenarios need to be as reliable as possible, the performance of these systems has to be evaluated. Field-tests in man oeuvres may be the preferred evaluation method. However, they are expensive, as sufficient hardware is needed. Furthermore, the results concerning some characteristics (e.g., scalability) are limited – who can perform Field-tests with several hundreds of devices? Thus, especially for the evaluation of algorithms and protocols, simulation is an alternative. Currently, there are two categories of wireless networks, namely, infrastructure-based wireless networks and mobile ad hoc networks.

Only if the fixed configuration portion (infrastructure) has been set up properly, can mobile users exchange information and share the service of the network. To overcome the limitations of such kind of infrastructure, mobile ad hoc networks are presented for mobile users with more flexibility and freedom.

As tactical networks may also be networks without infrastructure, the individual nodes and there movement characteristics need to be modeled. In this paper we will focus on models that realize the movement of individual nodes (microscopic models). In the literature there are already some surveys on mobility models. However, these surveys are quite old or miss a lot of specific models. Furthermore, there is no review concerning the requirements for tactical scenarios. Thus, in this paper we will give a survey on existing mobility models and classify and review these models concerning the requirements of tactical communication systems.

## II. COOPERATION AND SECURITY ISSUES IN MOBILE AD-HOC NETWORK

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific trade-offs between security and resource consumption of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently. Self-organization is a key property of ad-hoc networks. They cannot rely on central authorities and infrastructures, e.g. for key management. Latency is inherently increased in wireless multi-hop networks, rendering message exchange for security more expensive. Multiple paths are likely to be available. This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding.

Besides authentication, confidentiality, integrity, availability, access control, and no repudiation being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as location confidentiality, cooperation fairness and the absence of traffic diversion.

ISBN: 978-93-83758-09-8

The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers special opportunities to attackers. Without proper security, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior; preventing someone else from getting proper service, extracting data to get confidential information, and so on. Routes should be advertised and set up adhering to the routing protocol chosen and should truthfully reflect the knowledge of the topology of the network. By diverting the traffic towards or away from a node, incorrect forwarding, no forwarding at all, or other non-cooperative behavior, nodes can attack the network.

## III. BASIC IDEA OF PROPOSED SOLUTIONS

### *3.1 Preventing Mechanism*

Authentication by 'imprinting'. Stajano and Anderson authenticate users by 'imprinting' in analogy to ducklings acknowledging the first moving subject they see as their mother, but enable the devices to be imprinted several times. Imprinting is realized by accepting a symmetric encryption key from the first device that sends such a key. They neither address routing nor forwarding, however, are user authentication and authorization an important prerequisite for trust in the network layer also in mobile ad-hoc networks.

Asynchronous threshold security has been employed by Zhou and Haas together with share refreshing for distributed certification authorities for key management in mobile ad-hoc networks. They take advantage of inherent redundancies in such networks due to multiple routes to enable diversity coding, allowing for Byzantine failures given by several corrupted nodes or collusions. This approach potentially is a strong prevention mechanism, however, to the best of our knowledge, the impact on the network and the security performance remain to be investigated.

Incentives to cooperate have been proposed by Butty´an and Hubaux in the form of so-called nuglets that serve as a per-hop payment in every packet or in the form of counters to encourage forwarding. Both nuglets and counters reside in a secure module in each node, are incremented when nodes forward for others and decremented when they send packets for themselves. One of their findings is that, given such a module, increased cooperation is beneficial not only for the entire network but also for individual nodes.

Self-organized PGP by using chains of certificates has been developed by Hubaux, Butty´an and Capcun. Several certificate paths can be found by sharing information of nodes that each keep a small part of the certification knowledge, a prerequisite being the assumption that trust is transitive.

Localized certification based on the public key infrastructure (PKI) with certification authority and secret-share update functionalities distributed among neighbors have been suggested by Kong, Zerfos, Luo, Lu and Zhang. For threshold secret-sharing and certification nodes need K one-hop neighbors within a given time window. The nodes locally store the system certification revocation list. A simulation showed a good success ratio and tolerable delay.

SRP, the Secure Routing Protocol by Papadimitratos and Haas, guarantees correct route discovery, so that fabricated, compromised, or replayed route replies are rejected or never reach the route requester. SRP assumes a security association between end-points of a path only, so intermediate nodes do not have to be trusted for the route discovery. This is achieved by requiring that the request along with a unique random query indentifier reach the destination, where a route reply is constructed and a message authentication code is computed over the path and returned to the source. The correctness of the protocol is proven analytically.

ARIADNE, a secure on-demand routing protocol by Hu, Perrig, and Johnson, prevents attackers from tampering with uncompromised routes consisting of uncompromised nodes. It is based on Dynamic Source Routing (DSR) and relies on symmetric cryptography only. It uses a key management protocol called TESLA that relies on synchronized clocks. Simulations have shown that the performance is close to DSR without optimizations.

SEAD, Secure Efficient Distance vector routing for mobile ad-hoc networks by Hu, Johnson and Perrig is based on the design of destination-sequenced distance-vector routing (DSDV) and uses one-way hash functions to prevent uncoordinated attackers from creating incorrect routing state in another node. Performance evaluation has shown that SEAD outperforms DSDV-SQ in terms of packet delivery ratio, but SEAD adds overhead and latency to the network.

### *3.2 Reaction and Detection*

Intrusion detection for wireless ad-hoc networks has been proposed by Zhang and Lee to complement intrusion-prevention techniques. The authors argue that an architecture for intrusion detection should be distributed and cooperative, using statistical anomaly-detection approaches and integrating intrusion-detection information from several networking layers. They use a majority voting mechanism to classify behavior by consensus. Responses include re-authentication or isolation of compromised nodes. Detection rates and performance penalties remain to be investigated.

ISBN: 978-93-83758-09-8

Watchdog and pathrater components to mitigate routing misbehavior have been proposed by Marti, Giuli, Lai and Baker. They observed increased throughput in mobile ad-hoc networks by complementing DSR with a *watchdog* for detection of denied packet forwarding and a *pathrater* for trust management and routing policy rating every path used, which enable nodes to avoid malicious nodes in their routes as a reaction. Although this reaction does not punish malicious nodes that do not cooperate and actually relieves them of the burden of forwarding for others while having their messages forwarded, it allows nodes to use better paths and thus to increase their throughput.

CONFIDANT stands for 'Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks' and it detects malicious nodes by means of observation or reports about several types of attacks and thus allows nodes to route around misbehaved nodes and to isolate them from the network. Nodes have a *monitor* for observations, *reputation records* for first-hand and trusted second-hand observations, *trust records* to control trust given to received warnings, and a *path manager* for nodes to adapt their behavior according to reputation. Simulations for "no forwarding" have shown that CONFIDANT can cope well even with half of the network population acting maliciously.

CORE, a collaborative reputation mechanism proposed by Michiardi and Molva, also has a *watchdog* component; however it is complemented by a sophisticated reputation mechanism that differentiates between subjective reputation (observations), indirect reputation (positive reports by others), and functional reputation (task-specific behavior), which are weighted for a combined reputation value that is used to make decisions about cooperation or gradual isolation of a node. Reputation values are obtained by regarding nodes as requesters and providers, and comparing the expected result to the actually obtained result of a request. A performance analysis by simulation is stated for future work.

## IV. CONCLUSION

Mobile ad-hoc networks are vulnerable to attacks that differ from those in fixed networks; their properties pose additional requirements to security and cooperation protocols. There are many open research challenges, because by definition mobile ad-hoc networks are self-organized and have no infrastructure and central authorities. Examples for research questions are self-organized key management, cooperation incentives, group-membership and access control, authentication and identity persistence, and trust management.

## 5. REFERENCES

[1]. Vasudevan, S., Kurose, J, Towsley, D. Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks. Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP) (2004) 350-360

[2] Y. Afek and A. Bremler. Self-stabilizing unidirectional network algorithms by power supply. Chicago Journal of Theoretical Computer Science, December 1998.

[3] O. Bayazit, J. Lien, and N. Amato. Better group behaviors in complex environments using global roadmaps. 8th International Conference on the Simulation and Synthesis of living systems (Alife '02), Sydney, NSW, Australia, pp. 362- 370, December 2002.

[4] B. DeCleene et al. Secure group communication for Wireless Networks. In proceedings of MILCOM 2001, VA, October 2001

[5] C. Perkins and E. Royer. Ad-hoc On-Demand Distance Vector Routing. In proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999,pp. 90-100

[6] W. Heinzelman, A. Chandrakasan and H. Balakrishnan. Energy-Efficient Communication Protocol for Wireless Micro sensor networks. In proceedings of Hawaiian International Conference on Systems Science, January 2000.

[7] N. Malpani, J. Welch and N. Vaidya. Leader election Algorithms for Mobile Ad Hoc Networks. In fourth International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Boston, MA, August 2000.

[8] N. Lynch. Distributed Algorithms. 1996, Morgan Kaufmann Publishers, Inc.

[9] R. Gallager, P. Humblet and P. Humblet and P. Spira. A Distributed Algorithm for Minimum Weight Spanning Trees. In ACM Transactions on Programming Languages and Systems, vol.4, no.1, pages 66-77, January 1983.

[10] D. Peleg. Time Optimal Leader Election in General Networks . In journal of Parallel and Distributed Computing, vol.8, no.1, pages 96-99, January 1990.