A Novel Methodology for Securing Ad Hoc Network by Friendly Group Model

Md. Amir Khusru Akhtar and G. Sahoo

Abstract MANETs may be considered as a society in which nodes agree to cooperate with each other to fulfill the common goal. But noncooperation is genuine to save itself in terms of their battery power and bandwidth. Ad hoc network is still a challenge as lots of work has been proposed but they have serious limitations in terms of routing overhead and attacks. Modification of routing information's can be handled by secure routing protocols but non cooperation is still in its natal stage. Our proposed FG Model minimizes resource utilization by cutting down the routing overhead, so that less number of nodes participates in routing activities by creating smaller friendly groups. The proposed method minimizes routing overhead to a ratio of k: $1|k > 1$ (where k is the no. of friendly groups) and it can be implemented on the existing MNAET routing protocol (e.g., DSR, AODV and TORA).

Keywords Open MANET · Closed MANET · Friendly groups · Cooperative society · Border node · Regular node · Gateway

1 Introduction

Ad hoc wireless networks are infrastructure-less, self-organized network that can be created in minimum time. Cooperation is the backbone of such type of network because they have surplus responsibilities such as routing & addressing. In spite of

M. A. K. Akhtar (✉)
Department of Computer Science and Engineering,
ICFAI University, Ranchi, Jharkhand, India
e-mail: akru2008@gmail.com

G. Sahoo
Department of Information Technology, Birla Institute of Technology,
Mesra, Ranchi, Jharkhand, India
e-mail: gsahoo@bitmesra.ac.in

N. Chaki et al. (eds.), *Computer Networks & Communications (NetCom)*,
Lecture Notes in Electrical Engineering 131, DOI: 10.1007/978-1-4614-6154-8_3,

that nodes are free to move in the network without loosing connection. MANETS are difficult to implement due to their distributed and dynamic nature. A Protection model characteristic is not only to protect the existing attacks (malicious and selfish) but it should also minimize the routing overhead. MANET is the only option for many applications such as Military and Law, Disaster relief operations, Mine site operations and other suitable domain when infrastructures are not available, impractical, or expensive.

A MANET is a network of cooperation but when a node showing its selfishness all cooperation agreement fails. Selfishness is natural behavior and it must not be denied, it is genuine. These honest causes (i.e., to save battery life, to save bandwidth) encourages nodes to become selfish. Existing MANET protocols can prevent to some extent but with a serious overhead that is sometimes similar to the cost if nodes are not selfish. It can't be prevented by rewarding [1] or by enforcing some complex calculation [2–5]. Defining some new way to confront from this problem, it in terms of minimizing the routing activities that saves battery life, so that the non ethical behavior will not take place up to the maximum extent.

The motivation behind our approach is that network partitioning can improve the overall network throughput that solves both the malicious and selfish attacks. In this work we are categorizing MANETs into closed MANET and open MANET. Closed MANETs works together for a common goal and therefore selfishness is not often expected because they have some defined objective as in Military or police exercises, Disaster relief operations, and Mine site operations. On the other hand open MANETs are formed for diverse goals, they agree to share resource but for saving itself they may become selfish even though they don't like this.

MANETs issues a new future for Business meetings, home networking or distributive communication and computing. Designing a complex prevention scheme or defining some detection and exclusion mechanism for discouraging selfish behavior is not sufficient because still it consumes battery power and available bandwidth that is the real cause of selfishness.

Our proposed FG model divides a MANET of size N into k friendly groups with approx N/k number of nodes, which minimizes the throughput up to a ratio k: $1|k > 1$ where k represents number of groups. It consumes less battery power and bandwidth by minimizing the routing overhead this will establish a cooperative society for the successful execution of MANET.

The approach of this paper is organized as follows. Section 2 enlighten the related works in the field of selfish node prevention or detection and exclusion, and the impact of physical and virtual subnetting or partitioning in minimizing total routing overhead. Section 3 discusses the FG Model. Experimental analysis is given in Sect. 4. Section 5 addresses efficiency evaluation for reactive routing protocol with and without FG model. Finally Sect. 6 concludes the paper.

2 Related Work

Ad hoc network is still a challenge as lots of work has been proposed but they have serious limitations in terms of routing overhead and attacks. Modification of routing information's can be handled by secure routing protocols [6–10] but non cooperation is still a challenge for the existing secured routing protocols. A variety of routing protocols have been proposed but selfishness is still in its natal stage.

Works done on the area of detection of misbehavior using Reputation based mechanism are as follows.

"Watchdog" and "Pathrater" [1] mechanism was proposed to be used over the DSR [11] routing protocol but selfish nodes are rewarded because there is no punishment for the same. It has another serious drawback that extra battery power consumption because every node has to constantly listen to the medium.

CONFIDANT, "Cooperation of Nodes: Fairness In Dynamic Ad-hoc Networks" [2]. It has four components (a monitor, a reputation system, a path manager, and a trust manager) to achieve cooperation between nodes, but these four components are implemented in every node, as it creates lots of overhead.

CORE, "a collaborative reputation mechanism" [3], it uses Watchdog for monitoring mechanism with a reputation table. This mechanism punishes the selfish nodes but it is also very costly.

Friends & Foes [4] in which friend receives the services and Foes that is refuses to serve by the nodes. This method provide solution but with memory and message overhead.

RIW [5] this method gives emphasis is given on current feedback items rather than old ones. It keeps a node behaving selfishly for a long time after building up good reputation, but with impractical assumption.

Works done on the area of detection of misbehavior using Incentive based mechanism are as follows.

PPM/PTM [12] it uses two models the Packet Purse Model that loads Nuglets into data packets before sending them for the payment to intermediate nodes. Intermediate nodes can take more Nuglets than they deserve, and Packet Trade Model that maintains intermediate nodes trade packets with the previous node, and the destination finally pays the price of the packets. This model needs a secure hardware to keep nodes from tampering the amount of Nuglets.

Ad hoc VCG (Vickery, Clarke and Groves) [13] it has two phases the Route Discovery in which destination node computes needed payments for intermediate nodes and notifies it to the source node or the central bank, and Data Transmission phase where actual payment is performed. In VCG nodes totally depends on destination nodes report.

Sprite [14] works on Central Authorized Server (CCS). Nodes have to send a receipt to CCS for every packet they forward; CCS assigns credits to nodes according to the receipt. Scalability and message overhead are the major weaknesses.

Priority forwarding [15] uses two layered forwarding: Priced Priority forwarding and Free best-effort forwarding but it has packets forwarding problems.

PIFA (Protocol independent Fairness Algorithm) [16] is suitable for any routing protocol. It introduces Credit Manager (CM) that manages the credit databases for nodes, Bank Stations or sink nodes. Message processing overhead is the major weakness.

Game theory based schemes [17–19] and other schemes [20, 21] have weaknesses in terms of routing and processing overheads.

A Partition Network Model was proposed to minimize the routing overhead with Mobile agents [22]. This method minimizes overhead but not suitable for many applications.

For the minimization of routing overhead subnetting concepts was proposed [23] that uses a internet type structure in which the nodes are grouped into subnets acting as a single entity but it is difficult to apply due to their dynamic and distributed nature. It includes open challenges such as subnet formation and address acquisition, the intra-subnet routing and inter-subnet routing, and the mobility of nodes between subnets.

Some of the papers proposed efficient Virtual subnet model for MANET [24–26] but it is not suitable for devices having low computation power because each node in the subnet is authenticated using certificate and it involve so many computations.

3 Friendly Group Model (FG)

3.1 Overview

The proposed Friendly Group Model (FG) divides a MANET into a number of friendly groups, with one border group. Each friendly group consisting of regular nodes with one border node and it should be a member of the border group. The FGs are defined on the basis of common objectives.

Figure 1 shows our Friendly Group structure. The four different FGs are represented by cross, triangle, circle and square. In a FG Regular nodes are responsible for intra group routing while the border nodes are responsible for intra and inter group routing.

3.2 Elementary Terminologies

Definition 1. *Regular Node* (*RN*): *it represents a static or mobile terminal performs both terminal and routing functions within its friendly group.*

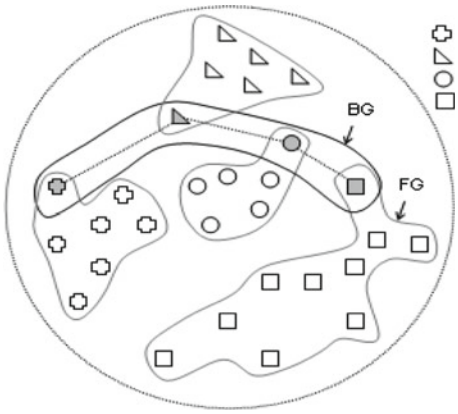

Fig. 1 Friendly group architecture of four FG with one BG

Definition 2. *Border Node* (*BN*): *it represents a static terminal performs terminal and routing functions within its friendly group and in the border group*.

Definition 3. *Closed MANET* (*CM*): *it represents a MANET containing set of nodes works together for common objectives*.

Definition 4. *OPEN MANET* (*OM*): *it represents a MANET containing set of nodes formed for diverse goals*.

Definition 5. *Friendly Group* (*FG*): *it represents a set of regular nodes together with one border node which has common objectives* (*Closed MANET*).

Definition 6. Border *Group* (*FG*): *it represents a set of border nodes used as gateways for the FGs which has diverse objectives* (*Open MANET*).

3.3 FG Components

Our approach involves the following FG components.

- Ad hoc Component: It includes ad hoc related protocols installed in nodes and connected with ad hoc networks.
- The border node must be equipped with two wireless devices to support multiple networks and similar concept was defined in [27]. The first NIC connected to the FG and the second NIC is connected to the BG as given in Fig. 2.

3.4 Group Formation

Some assumption has been taken for the grouping. To make a group a set of nodes form a FG in which nodes having common goal. For example employees of several

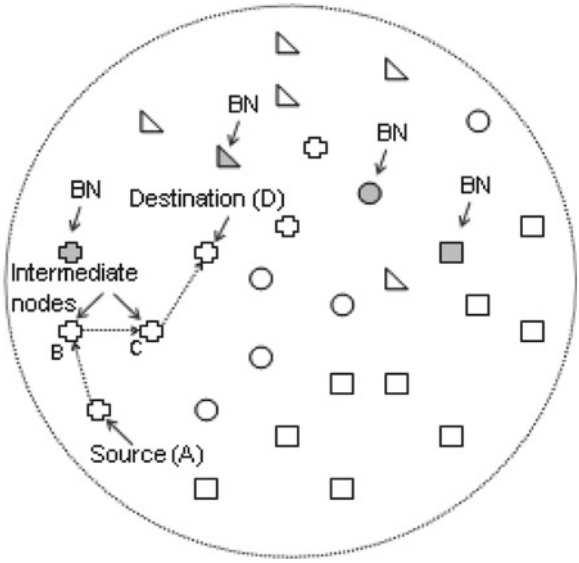

Fig. 2 Within group transmission

departments can be grouped into common objective groups like marketing (FG1), finance (FG2), HRD (FG3) and Personnel (FG4).

3.5 Transmission of Packets

3.5.1 Within a Friendly Group (Closed MANET)

Packet addressed to the same FG is forwarded to the destination using existing MANET routing protocol (e.g., DSR, AODV, and TORA) [11, 28, 29]. The intra group routing is given in Fig. 3.

Here node A is the source and node D is destination. The dotted arrow shows the data flow and the path is A $\rightarrow$ B $\rightarrow$ C $\rightarrow$ D. The routing operation will be performed without the help of BN. However, while routing, if BN node of same group participates in routing activities, then BN node would act like a RN.

3.5.2 Inter Group (Open MANET)

Packet addressed to a destination of other FG routed through the border node. The borders nodes are the gateway for FGs. BNs use MANET routing protocols (e.g., DSR,

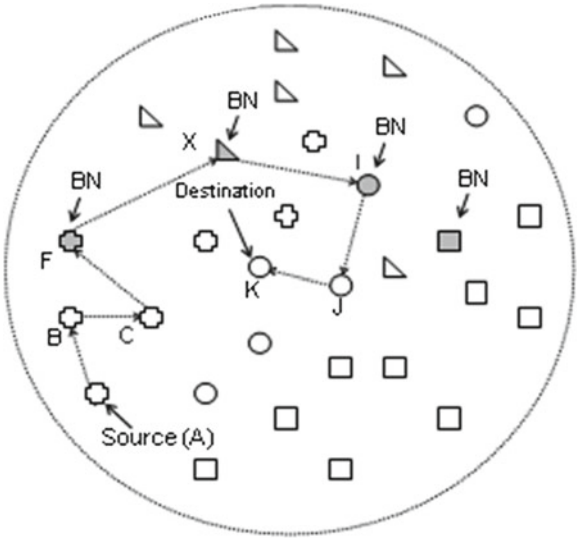

Fig. 3 Inter group transmission

AODV, and TORA) to send and receive packets. The inter group routing is given in Fig. 4.

Here, the source node is a cross node A and destination node is a circle node K. The dotted arrow data flow shows that packet is first forwarded to BN of the cross FG

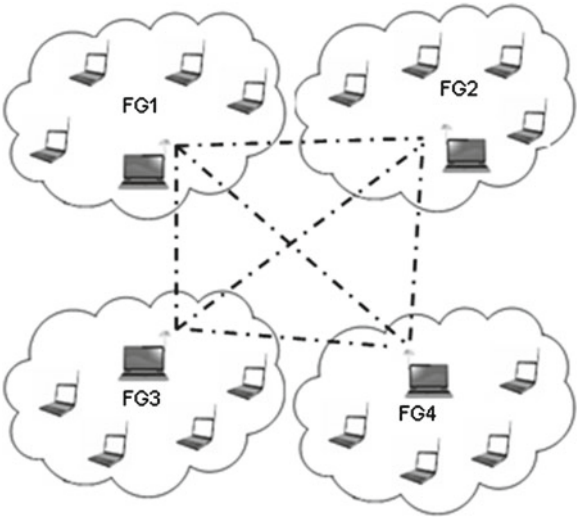

Fig. 4 Experiment overview

with path A → B → C → F. After receiving the packet the BN checks the packet to identify destination. If the destination is on other FG then border group routing will be performed to sends the packet to the destination. The complete flow from source to destination is shown by the dotted arrow and the packet travels the path A → B → C → F → X → I → J → K.

4 Experiments on Lab

4.1 Scenario Description

Figure 5 shows a scenario in which our proposal is based. We have deployed a Friendly group structure, over the Lab with 20 nodes. We select 4 nodes as the border nodes. RNs having single NIC and BNs are equipped with two NICs.

4.2 Regular Node Configuration

The RNs containing single NIC and it is connected to FG as given Fig. 6.

The RNs default gateway will be used when a destination IP address does not fall within the FG, and it is used to route packets to other group.

4.3 Border Node Configuration

The BN multiple NIC configurations are given in Fig. 2. The Border node is connected to a FG via NIC1 which allows routing and forwarding within group and NIC2 is connected to BG to provide inter routing.

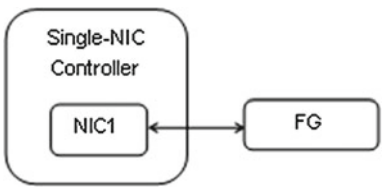

Fig. 5 RNs having single NIC controller

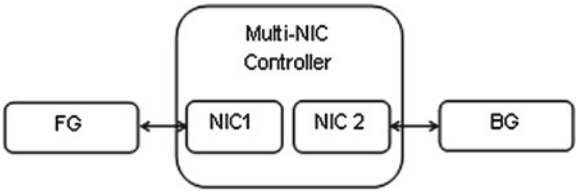

Fig. 6 BNs having multiple NIC controller

4.4 IP Structure

The FGs IP addresses in the range of 192.168.x.x with subnet mask 255.255.255.0 to NIC1. The default gateway address is 10.0.0.x for FGs. In this FG Model, only the NIC1 default gateway will be used because when a destination IP address does not fall within the FG of any NIC, then the default gateway of NIC1 is used to route packets to other group. The NIC2 default gateway should be blank because it routs the packets to the wrong network and causing them to be undeliverable.

The IP structure for FG Model is shown in Fig. 7 in which IP denotes internet protocol address and SM denotes Subnet Mask.

Fig. 7 FG IP structure

```
<?xml version="1.0" ?>
- <MANET>
  - <FG1>
    - <BN>
      - <NIC1>
          <IP>192.168.1.1</IP>
          <SM>255.255.255.0</SM>
          <Gateway>10.10.0.1</Gateway>
        </NIC1>
      - <NIC2>
          <IP>10.10.0.1</IP>
          <SM>255.0.0.0</SM>
          <Gateway>0.0.0.0(unspecified)</Gateway>
        </NIC2>
      </BN>
    - <RN1>
      - <NIC1>
          <IP>192.168.1.2</IP>
          <SM>255.255.255.0</SM>
          <Gateway>192.168.1.1</Gateway>
        </NIC1>
      </RN1>
    + <RN2>
    + <RN3>
    + <RN4>
    </FG1>
  + <FG2>
  + <FG3>
  + <FG4>
  </MANET>
```

4.5 Shifting of Node

Due to the dynamic nature of MANET the mobility of the nodes into the friendly group can be handled by MANET routing protocol. The mobile nodes need to discover the border node which is in the best coverage area of the FG.

5 Efficiency Evaluation

5.1 Overhead Comparisons

We have analyzed the overhead for reactive routing protocols [30], and the proposed subnetting concept [23] for a MANET that reduces routing overhead with some open challenges such as subnet formation and address acquisition, the intra-subnet routing and inter-subnet routing, and the mobility of nodes between subnets.

Our FG model is very simple because it can be implemented within a short time and it does not involve any further computations to enforce authentication. This model classify MANETs into open MANETs and closed MANETs and works efficiently using existing routing protocols. The classification minimizes total no. of control packets in routing activities.

The reduction of the routing information is achieved by partitioning the network into FGs and the FGs are joined using BG. This filtered the control packet overhead and our protocol assumes that inter group routing will happen rarely.

The overhead comparison between a reactive routing protocol and the same protocol with friendly Groups is given in Fig. 8. The result shows the reduction in control packets by introducing FGs. Our model divides a MANET of size N into k friendly groups with approx N/k number of nodes per group. The total control overhead in is N^2 with flat structure and in FG (Hierarchical) structure it N^2/k which minimizes the throughput up to a ratio k: $1|k > 1$.

5.2 Advantage of FG Model

This model uses two NIC instead of virtual subnetting [24–26] because of the following advantages:

- Simpler to design because it divides a MANET by involving NICs
- Cost effective because dividing a network by employing NICs is very cheaper
- Negligible performance overheads due to its design but in virtual subnetting nodes are authenticated using certificate that involve so many computations.
- Suitable for devices having low computation power because it does not involve any computations for authentication.

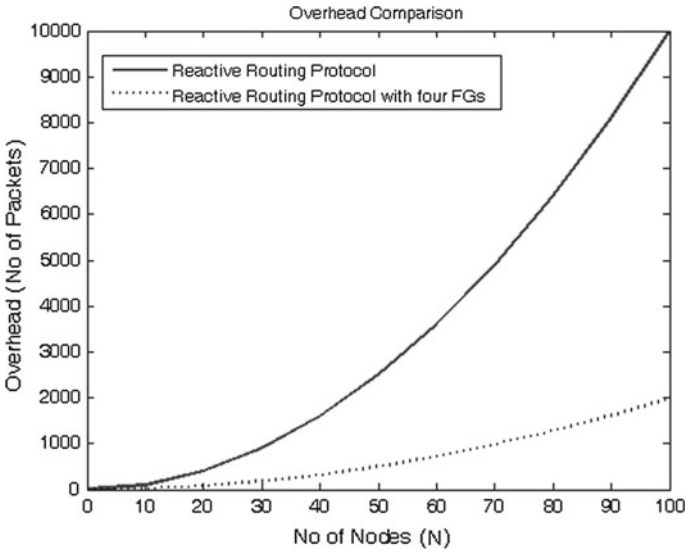

Fig. 8 overhead comparison between a reactive routing protocol and the same protocol with friendly Groups

6 Conclusion

Our Friendly Group Model for MANET will encourage nodes cooperation because it reduces the routing overhead. This model divides a MANET of size N into k friendly groups with approx N/k number of nodes, which minimizes the throughput up to a ratio k: $1|k > 1$ where k represents number of groups. This model saves battery life and bandwidth and thus enhances cooperation by eliminating the genuine cause of selfishness.

This model assumed that by saving battery power nodes have fewer chances for misbehaving and it is true also because they have enough energy to survive.

References

1. Marti S, Giuli TJ, Lai K, Baker M (2000) Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on mobile computing and networking (ACM MobiCom 2000). ACM, New York, pp 255–265
2. Buchegger S, Boudec J-YL (2002) Performance analysis of the CONFIDANT protocol: cooperation of nodes—fairness in distributed ad-hoc networks. In: MOBIHOC'02
3. Michiardi P, Molva R (2002) CORE: a collaborative reputation mechanism to enforce cooperation in mobile ad-hoc networks. In: CMS'2002, communication and multimedia security 2002 conference, 26–27 Sept 2002, Portoroz, Slovenia/Also published in the book : Advanced communications and multimedia security, Jerman-Blazic B, Klobucar T (eds), Kluwer Academic Publishers, Dordrecht, ISBN 1-4020-7206-6, Aug 2002, 320 pp

4. Miranda H, Rodrigues L (2003) Friends and foes: preventing selfishness in open mobile ad hoc networks. In: ICDCSW'03
5. Adams WJ, Hadjichristofi GC, Davis NJ IV (2005) Calculating a node's reputation in a mobile ad hoc network. In: Proceedings of IEEE international performance computing and communications conference (IPCCC), pp 303–307
6. Sanzgiri K, Dahill B, Levine B, Shields C, Belding-Royer E (2002) A secure routing protocol for ad hoc networks. In: 10th IEEE international conference on network protocols (ICNP), Nov 2002
7. Zapata MG, Asokan N (2002) SAODV: securing ad-hoc routing protocols. In: 2002 ACM workshop on wireless security (WiSe 2002), Sept 2002, pp 1–10
8. Hu Y, Perrig A, Johnson D (2002) Ariadne: a secure on-demand routing protocol for ad hoc networks. In: Proceedings of the eighth annual international conference on mobile computing and networking, Sept 2002, pp 12–23
9. Hu Y, Johnson D, Perrig A (2002) SEAD: secure efficient distance vector routing in mobile wireless ad hoc networks. In: Fourth IEEE workshop on mobile computing systems and applications, June 2002, pp 3–13
10. Papadimitratos P, Haas Z, Samar P (2002) The secure routing protocol (SRP) for ad hoc networks, internet-draft, draft-papadimitratos-securerouting-protocol-00.txt, Dec 2002
11. Johnson D, Maltz D, Hu Y-C (2003) The dynamic source routing protocol for mobile ad hoc networks (DSR). IEEE internet draft, Apr 2003
12. Buttyan L, Hubaux J (2000) Enforcing service availability in mobile ad hoc WANs. In: Proceedings of IEEE/ACM MobiHOC workshop
13. Anderegg L, Eidenbenz S (2003) Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In: Proceedings of ACM MobiCom 2003, pp 245–259
14. Zhong S, Chen J, Yang YR (April 2003) SPRITE: a simple, cheatproof, credit-based system for mobile ad-hoc networks. In: Proceedings of INFOCOM 03, pp 1987–1997, Apr 2003
15. Raghavan B, Snoeren AC (2003) Priority forwarding in adhoc networks with self-interested parties. In: Workshop on peer to peer systems, June 2003
16. Yoo Y, Ahn S, Agrawal DP (2005) A credit-payment scheme for packet forwarding fairness in mobile MANETs. In: Proceedings of IEEE ICC
17. Srinivasan V, Nuggehalli P, Chiasserini CF, Rao RR (2003) Cooperation in wireless MANETs. In: Proceedings of IEEE INFOCOM
18. Mahajan R, Rodrig M, Wetherall D, Zahorjan J (2005) Sustaining cooperation in multi-hop wireless networks. In: Proceedings of NSDI
19. Hales D (2004) From selfish nodes to cooperative networks—emergent link-based incentives in peer-to-peer networks. In: Proceedings of IEEE international conference on peer-to-peer computing, pp. 151–158
20. Yang H, Meng X, Lu S (2002) Self-organized network-layer security in mobile ad hoc networks. In: Proceedings of the ACM workshop on wireless security. ACM, New York, pp 11–20
21. Feigenbaum J, Papadimitriou C, Sami R, Shenker S (2002) A BGP based mechanism for lowest-cost routing. In: Proceedings of the 21st annual symposium on principles of distributed computing. ACM, New York, pp 173–182
22. Chiang T-C, Tsai H-M, Huang Y-M (2005) A partition network model for ad hoc networks. In: Wireless and mobile computing, networking and communications (WiMob'2005), pp 467–472
23. López J, Barceló JM, García-Vidal J (2006) Subnet formation and address allocation approach for a routing with subnets scheme in MANETs. In: Wireless systems and network architectures in next generation internet. Lecture notes in computer science, vol 3883/2006, pp 62–77. DOI:10.1007/11750673_6
24. Chowdhury MAH, Ikram M, Kim K-H (2008) Secure and survivable group communication over MANET using CRTDH based on a virtual subnet model. In: IEEE Asia-Pacific services computing conference
25. Chang C-W, Yeh C-H, Tsai C-D (2010) An efficient authentication protocol for virtual subnets on mobile ad hoc networks. In: International symposium on computer, communication, control and automation

26. Vilhekar AA, Jaidhar CD (2012) Modified authentication protocol using C mobile adhoc networks. In: Wireless communications and applications. Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 72. Springer, Berlin, pp 426–432
27. National Instruments, www.ni.com/white-paper/12558/en. Accessed 06 June 2012
28. Perkins C, Royer EB, Das S (2003) Ad hoc on-demand distance vector (AODV) routing. IETF internet draft
29. Park V, Corson S (2001) Temporally ordered routing algorithm (TORA). IETF internet draft
30. Viennot L, Jacquet P, Clausen TH (2004) Analyzing control traffic overhead versus mobility and data traffic activity in mobile ad-hoc network protocols. Presented at ACM wireless networks journal (Winet)