Sindh Univ. Res. Jour. (Sci. Ser.) Vol.43 (1-A) 91-96 (2011)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

COINS: Towards a Correlation Based Intrusion Detection System for Mobile Ad hoc Network

N. Islam[1], Z. A. Shaikh[1] and Aqeel-ur-Rehman[2]

[1,]National University of Computer and Emerging Sciences, Karachi, Pakistan
[2]Hamdard University, Karachi, Pakistan
noman.islam@nu.edu.pk; zubair.shaikh@nu.edu.pk; aqeel.rehman@nu.edu.pk
Corre
rev

Abstract: Mobile Ad-hoc Networks (MANET) encounters significant amount of security challenges due to their peculiar properties. To address these security challenges, this paper presents an approach towards secure data management in MANET. It presents an ingenious strategy based on the relationships among data items discovered via association rules mining algorithm. The proposed strategy assumes that the requests propounded by a particular host in a session are dependent on their underlying relationships and digression from these relationships should be regarded as abnormalcy. Based on this theory, a Correlation Based Intrusion Detection System (COINS) for MANET has been presented. The proposed solution considers the associations among requests of a session to establish the integrity of session and consequently of the data consumers. An analysis of the proposed scheme has been done under different scenarios that signifies the effectiveness of the proposed scheme.

Keywords- Correlation; MANET; IDS; Security; Secure Data Management

INTRODUCTION

A. *Problem Introduction*

Mobile Ad hoc Networks are characterized as infrastructure-less network $G(N,E)$ with a set of nodes $N=\{n_1,n_2,n_3,\ldots\}$ and a set of links $E=\{e_1,e_2,e_3,\ldots\}$ and $e_i \in N\times N$. The infrastructure-less nature of MANET and effort-less deployment foster a range of potential applications (Shaikh 2008; Shaikh et al., 2008; Shaikh *et al.*, 2010).

Table 1: A Summary of Research Issues of MANET

Problem	***Issues / Description***	***Solutions***
Power Management	low powered battery	exploits various modes of battery i.e. doze, sleep, active
Routing	stale routes routing loops	AODV DSR DSDV
QoS	links instability	Coordinated Effort at all layers, (Brahma, Kim *et al.*, 2005)
Addressing	no DHCP DoS attack on address spaces	Mobile IP
Transport Protocol	frequent link failure considered as congestion	TCP variants
Security	open for all no dedicated security servers alien environment	Threshold cryptography IDS
MAC Layer	hidden node problem exposed node problem	(Brahma, Kim, *et al.* , 2005)

However, the flexibility of the MANET comes with the onset of an array of newer challenges. These challenges are because of the improvised nature, low resources, heterogeneous temperament etc. As a result, various academic and research circles are actively involved in addressing various issues of MANET. These research issues consist of physical layer issues (i.e. MAC Layer protocols, power management), communication layer (i.e. routing, transport protocols) and application layer issues (i.e. service discovery, query processing) etc. **(Table 1)** provides a summary of these features of MANET.

Among the issues discussed in table 1, security is considered as the essential component of any MANET application. There have been a number of customary solutions for providing security in conventional systems. These solutions include cryptographic algorithms, hashing schemes, message authentication codes etc. However, these old techniques can't be simply plugged in MANET environments. These algorithms tumbles in MANET because of the its dynamic and infrastructure-less environment. The resource constrained and unreliable mobile nodes also pose considerable challenges. Additionally, unstable and asymmetric links of MANET demands proper attention towards the design of any security algorithm for MANET. **(Table 2)** summarizes these security challenges of MANET in contrast with the traditional systems.

The objective of this paper is to provide a secure data management solution for MANET. Data Management is a set of mechanisms essential to ensure that the end user can consume the data it desires in pervasive fashion.

Table 2: Security Challenges in MANET

Characteristics	*Conventional Network*	*MANET*
Nodes Characteristics		
Mobility	–	+
Resource	+	–
Reliability	+	–
Links Characteristics		
Links		
Bandwidth	+	–
Symmetry	+	–
Stability	+	–
Environment Characteristics		
Environment		
Dynamism	–	+
Infrastructure	+	–
Certification Authority	+	–
DHCP	+	–
Interoperability	+	–
Nodes Acquaintance	+	–

Formally, if $D=\{d_1,d_2,d_3,\ldots\}$ represents the set of data prevailing on the network and Σ represents the alphabet i.e. $d_i \in \Sigma$, then data management is defined as:

$$data\ management = \{\alpha(D_i): D_i \subseteq D\} \quad (1)$$

In MANET, the problem of providing security of data management operations is not a straightforward job because of the new challenges that arise in MANET as mentioned in table II. To cope with these challenges, this paper presents a security solution by extending our earlier proposed data management solution(Islam 2008; Islam and Shaikh 2008; Islam and Shaikh 2009; Islam, Shaikh *et al.,* 2010). The solution is an Intrusion Detection System based on the isolation of an intruding node from the network considering the data requests made by the particular node. Let f_S signifies a function that defines the character of a node i on the basis of its requests $d_{ij}' \in D$. Then f_s can be expressed as:

$$f_1 S: D(\{normal, malicious\} \quad (2)$$

The function f_s identifies a misbehaving node on the network based on its activities deviating from the normal pattern. The normal patterns are determined by applying association rules mining algorithm on the past requests made by all the nodes of the network. Before proceeding towards the details, we will first present the literature related to our work.

B. Literature Review

(Fig. 1) highlights the current research work on security in MANET that includes: protecting MAC layer, secure routing Intrusion Detection System and cryptographic scheme. At the link layer, a number of approaches like extensions to IEEE 802.11 MAC (Kyasanur and Vaidya 2003) and IEEE 802.11 WEP have been proposed (IEEE 2002). As routing layer of MANET is vulnerable to a range of security attacks, a number of secure routing protocols have been proposed at the networking layer. This includes (Michiardi and Molva 2004): Secure Routing Protocol, ARIADNE, ARAN and SEAD etc. A number of public and private key cryptographic security schemes are also cited in literature (Luo and Lu 2002; Capkun, Buttyán *et al.,* 2003). In (Zhou and Haas 2002), a threshold cryptography based approach has been presented for key management in MANET.

Intrusion Detection System (IDS) is another way of protection that recognizes a vicious entity on the network based on known signature patterns (misuse detection) or user's activities (anomaly detection) (Zhang and Lee 2000; Anantvalee and Wu 2007). In (Shaikh 2007) an IDS security architecture based on Mobile Agents is proposed. The authors employ various types of mobile agents for topology management and intruder's identification etc. A centralized entity is elected from the participating nodes on the network that launches a mobile agent upon onset of any node on the network. The mobile agent performs various security checks on the new host to confirm this node as a well-behaving node and then grants network access to this node. In (Yan, *et al.,* 2004) an IDS solution by establishing a correspondence with human immune system is offered. Mobile Agents are launched similar to antibodies in human systems upon arrival of any unrecognized entity on the network. In (Lee, *et al.,* 2003) a cooperative intrusion detection scheme has been proposed that identifies anomalies by a node in the network based on pattern classification techniques.

As far as the data management frameworks are concerned, it includes: MoGATU (Joshi, *et al.,* 2006), DRIVE (Xu and Wolfson 2005) and (Islam 2008; and Shaikh 2008; and Shaikh 2009; Shaikh *et al.,*2010). MoGATU is a data management framework based on the cross-layer mechanisms that addresses various issues of data management like discovery, caching, query processing and security etc. In (Perich, *et al.,* 2006; Joshi, *et al.,* 2006), a trust management scheme is

proposed for MoGATU based on query packs that embraces information about reliable data sources and mechanisms to identify and react to malicious activity in proactive and reactive fashion. DRIVE(Xu and Wolfson 2005) is an incentive based opportunistic approach to data management system for vehicular environments. (Islam 2008; Shaikh 2008; and Shaikh 2009; Shaikh *et al.*, 2010) is a data management framework based on exploiting network layer capabilities and association rules mining for performing various aspects of data management. This paper extends this framework further by plugging a security module that exploits existing components for performing detection of an intruder on the network.

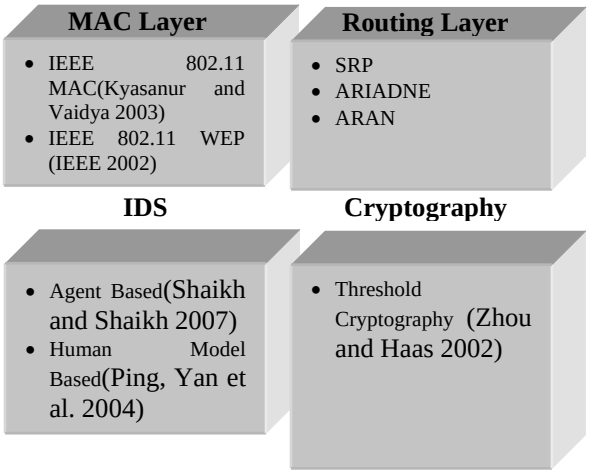


Fig. 1: A Summary of Security Approaches for MANET

MATERIALS AND METHOD

(Fig. 2) highlights the major component of our proposed data management framework where the proposed components for security are contrasted from existing components. There are a number of components like discovery, catalog, data mining, logging and correlation based security management etc. The *service discovery component* accomplishes the task of discovering the services, data and other resources from the network on the basis of a request floated by a consumer. The *service catalog* maintains the list of services/data/resources etc. available on the network. This also includes the meta-information to describe the services hosted by the node. The *log database* has the history of requests issued by consumers in the past in the form of sessions. A *session* can be defined as data requests in a sequence posed by a data consumer. A session H_i maintained by a node n_i can be expressed as:

$$H_i = \left\{ d'_{ij} : (j = 0) \; or \; \left(d'_{ij}.t - d'_{ij} - 1.t < \varepsilon_1 \right) \right\} \quad (3)$$

where, ε_1 represents a small threshold and $d_{ij}'.t$ represents the time of issuance of the request $d_{ij}.t$. The log database L can be represented as:

$$L = \{H_1, H_2, H_3, \ldots\} \quad (4)$$

The log database is used by *association rules mining component* to calculate the correlation among data items. This correlation is used by the component COINS to establish the request patterns of a normal behaving nodes and thus a misbehaving node can be identified on the basis of their request sessions.

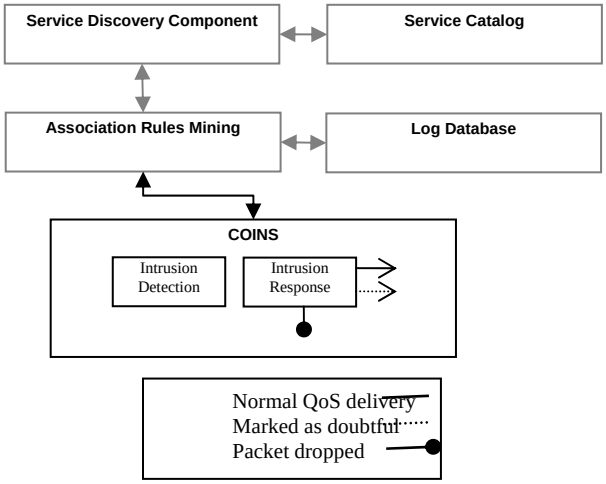


Fig. 2: Block Diagram illustraing the propsed scheme

COINS component itself comprises of two sub-components: the intrusion detection and intrusion response components that are used for descrying and penalizing intruders on the network.

C. Intrusion Detection Component (IDC)

The *Intrusion Detection Component (IDC)* is responsible for recognizing intruding activities on the network. IDC works by calculating the *deviation count* for a particular session. If the deviation count gets above a particular threshold, integrity of the session becomes questionable.

Let *dc* denotes the deviation count of a request session $H_i=\{d_{i1},d_{i2},d_{i3},\ldots,d_{ih}\}$. For a particular request d_{ij}', the deviation count can be estimated by the intrusion detection component as follows:

$$dc = \begin{cases} dc & if \; \rho\left(d_{i1}, d_{i2}, \ldots, d_{ih}, d'_{ij}\right) > \varepsilon_2 \\ dc + 1 & otherwise \end{cases} \quad (5)$$

where, $\rho(a, b)$ denotes the correlation between *a* and *b*. ε_{s_1} represents a threshold value. The deviation count is an estimate of how much a particular session behaves differently from the sessions maintained by other nodes in the past. If a particular session deviation count exceeds a threshold ε_{s_2}, the session can be marked as a malicious and the owner of the session can be regarded a malicious node. The integrity of session *I* estimated by the intrusion detection module can thus be expressed as follows:

$$I(H) = \begin{cases} normal & if\ dc < \varepsilon_{s_2} \\ malicious & otherwise \end{cases} \quad (6)$$

```
class DataManagement {
        ServiceDiscoveryComponent discovery;
        AssociationRulesMining mining;
        LogDatabase log;
        ServiceCatalog catalog;
        COINS coins;

        public DataManagement() {
           //start various components
           …
           coins = new COINS();
        }

        public void dataRequest(Request d){
           coins.applySecurityCheck(d);
           log.logDataRequest(d);
           If(!catalog.contains (d)) {
                discovery.discover(d);
           }
            // consume requested item
           …
        }

        class COINS {
                Hashtable dc = new Hashtable();
                Hashtable sessionHistory = ne wHashtable();
                public void applySecurityCheck (Request d) {
                    // for a new consumer, a new session is created
                    If(dc.get(d.consumer) == null) {
                          dc.put(d.consumer,0);
                     }
                     sessionHistory.put(d.consumer,d);
                     if
        (!mining.MiningResults.contains(sessionHistory)) {
                          int old_dc = dc.get(d.consumer);
                          old_dc++;
                          dc.put(d.consumer,old_dc);
                     }
                    if(dc.get(d.consumer) > threshold) {
                       //signal an intruding session
                       Message m = new Message();
                       m.setText("consumer" + d.consumer + "is an
        intruder");
                       send(m, getAdjoiningNodes());
                       performIntrusionResponse();
                    }
                }
        }
}
```

Fig. 3: Pseudo Code illustrating the working of COINS

D. Intrusion Response

The *Intrusion Response Component (IRC)* has the job of countering any type of intrusion in the network. One of the key properties of MANET is multi-hop routing. The response component works by simply ignoring the packets of any malicious nodes thus isolating the malicious node from the network. It operates in three modes: QoS packet delivery, packet marking and packet dropping. For a well-behaving node, it forwards the packet using simple QoS based delivery mechanism. In case of any doubtful node, it can mark the packet as of skeptical nature, while for an intruding node, its packet can simply be dropped. **(Fig. 3)** describes the working of proposed security scheme. Upon instantiation, the *DataManagement* class starts it's various sub-components (e.g. log database, mining etc.). The *dataRequest* method outlines how a request for any data item is handled by the data management component. It first performs the security measures by calling the *applySecuirtyCheck* method of COINS. It the request passes all security checks, it is logged and corresponding response is generated. The *COINS* class sketches the working of our proposed security scheme. The hash table *dc* maintains the deviation count of various consumers where as the hash table *sessionhistory* maintains the requests made by a particular consumer in a session. The method *applySecurityCheck* performs various security checks to confirm the integrity of session. It compares the session history of the request's consumer with the mining results computed by the mining component. If there is no similar pattern found, it is regarded as intrusion and a message is sent to adjacent nodes on the network.

3	4	5	7	
3	4	5	8	
4	5	7	8	
3	5	7	8	
3	4	6	10	
6	7	8	10	
6	10	11	12	13

a: Frequent Item sets

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0
4	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0
5	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0
6	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0
7	0	0	1	1	1	1	0	1	0	0	0	0	0	0	0
8	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
14	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

b: Correlation Matrix

Fig. 4: Frequent Item sets computed by FP-Growth Algorithm

RESULTS AND DISCUSSION

E. Results and Analysis

In this section, we will briefly analyze the effectiveness of COINS under Denial of Service (DOS) and provide the discussions on implementation. A thorough evaluation of the scheme is left as a future work. To evaluate the efficacy of proposal, FP-Growth Association Rules Mining algorithm(Islam and Shaikh 2009) has been applied on a campus data requests for You Tube videos*(Zink, Suh et al.,* 2008). **(Fig. 4)** illustrates some of the frequent item sets discovered by the algorithm. Suppose the threshold value is 5. Let $\sum$={1,2,3,…,13} and $a,b \in \sum$. Following cases analyze the behavior of COINS under various types of attacks.

Case 1 (Sequence Repeat):

Let the intruder floats the queries with the following pattern:

(a . b) *

Let a=3 and b=4, then following is the response of COINS:

Request	DC	Response
3	0	
3 4	0	
3 4 3	1	
3 4 3 4	2	
3 4 3 4 3	3	
3 4 3 4 3 4	4	
3 4 3 4 3 4 3	5	malicious session detected

Case 2 (Selective Repeat):

Let the intruder floats the queries with the following pattern:

(a | b) *

If a=3 and b=4, following is the response of COINS:

Request	DC	Response
3	0	
3 4	0	
3 4 4	1	
3 4 4 3	2	
3 4 4 3 4	3	
3 4 4 3 4 3	4	
3 4 4 3 4 3 3	5	malicious session detected

Case 3 (Random Repeat):

Let the intruder floats the queries on the basis of following pattern:

$\sum$*

Following is the response of COINS:

Request	DC	Response
3	0	
3 1	1	
3 1 2	2	
3 1 2 11	3	
3 1 2 11 5	3	
3 1 2 11 5 12	4	
3 1 2 11 5 12 13	5	malicious session detected

F. Discussions on Implementation

This paper presents an approach towards intrusion detection based on association rules mining algorithm. The paper provides a brief analysis of the scheme under few basic scenarios. However, a thorough investigation is necessary to truly validate the proposed scheme. We now present a brief discussion on the implementation aspects essential for a comprehensive evaluation of COINS.

A plenary examination of COINS primarily demands its implementation on a real world setup (e.g. (Perich, Joshi *et al.*, 2006) (Xu and Wolfson 2005) and (SunMicrosystems 2001) etc.) or a in a simulation environment (e.g. JIST (Barr, Haas *et al.*,2004)). The second question is the implementation of various sub-components of COINS. This includes the selection of appropriate data structures and algorithms for service discovery, caching and logging etc. Some of these aspects have been highlighted in (Shaikh *et al.*,2008; Shaikh *et al.*, 2009; Shaikh *et al.*,2010) etc.

For an intensive inquiry of COINS, its responses under various types of security attacks like DDOS attacks, Worm Hole attacks, Black Hole attacks, Rushing attacks and Jelly Fish attacks etc. must be investigated. The signatures of these attacks can be utilized to generate malicious sessions and the response of COINS can be observed against these attacks. In particular, the proportion of false intrusion alarm (i.e. the identification of a node as intruder when it is a well-behaving node) should be examined.

CONCLUSION

We fold the discussion by pointing out some of the areas where further research can be sought. The existing association rules mining algorithm has high computational and memory demands. In this regards, approximate algorithms can be crafted that can cope with the minimal resources of the node and also tells the correlation among data items. The proposed intrusion response module also demands further deliberation and analysis. The researchers can also steer their efforts towards the exploitation of correlation information for other operations of data management like replication, query processing and optimization, etc.

ACKNOWLEDGMENT

This manuscript is an extended version of our earlier paper that has been published in proceedings of conference “International Conference on Computers & Emerging Technologies” (ICCET 2011), that was held on 22-23 April 2011 at Shah Abdul Latif University, Khairpur, Sindh, Pakistan. We would also like to acknowledge Higher Education Commission (HEC), Pakistan for their support in this research work.

REFERENCES

Abbasi, A. Z. and Z. A. Shaikh (2008) "Building a Smart University Using RFID Technology". International Conference on Computer Science and Software Engineering (CSSE 2008), Wuhan, China.

Anantvalee, T. and J. Wu (2007) "A survey on intrusion detection in mobile ad hoc networks." Wireless Network Security: 159-180.

Aqeel-ur-Rehman, Z. A. Shaikh, (2010) "An Integrated Framework to Develop Context--Aware Sensor Grid for Agriculture." Australian Journal of Basic and Applied Sciences **4**(5): 922-931.

Barr, R., Z. J. Haas, (2004) "JIST: Embedding simulation time into a virtual machine". EuroSim Congress on Modelling and Simulation.

Brahma, M., K. W. Kim, (2005) "A new approach for supporting QoS in MAC layer over MANETs". Systems Communications, Montreal, Canada.

Capkun, S., L. Buttyán, (2003) "Self-organized public-key management for mobile ad hoc networks." IEEE Transactions on mobile computing: 52-64.

IEEE (2002) "Wireless Medium Access Control and Physical Layer (PHY) Specifications: Specification for Enhanced Security." IEEE Std. 802.11i/D30.

Islam, N. (2008) "A Data Management Framework for Mobile Ad hoc Networks (MANET)". Doctoral Symposium on Research in Computer Science, University of Central Punjab, Lahore, Pakistan.

Islam, N., G. A. Mallah, (2010) "FIPA and MASIF standards: a comparative study and strategies for integration". National Software Engineering Conference, Rawalpindi, Pakistan, ACM.

Islam, N., N. A. Shaikh, (2010) "A Network Layer Service Discovery Approach for Mobile Ad hoc Network Using Association Rules Mining." Australian Journal of Basic and Applied Sciences **4**(6): 1305-1315.

Islam, N. and Z. A. Shaikh (2008) "A Novel Approach to Service Discovery in Mobile Adhoc Network". International Networking and Communications Conference, Lahore University of Management and Science, Lahore, Pakistan.

Islam, N. and Z. A. Shaikh (2009) "Service Discovery in Mobile Ad hoc Networks Using Association Rules Mining". 13th IEEE International Multitopic Conference 2009 (INMIC-2009), Islamabad, Pakistan.

Islam, N., Z. A. Shaikh, (2008) "Towards a Grid-based approach to Traffic Routing in VANET". 8th IIEE-IEEE Student Branch Annual Student Seminar and Project Exhibition (E-Indus 2008) Institute of Industrial and Electronics Engineering, Karachi, Pakistan.

Kyasanur, P. and N. H. Vaidya (2003) "Detection and handling of MAC layer misbehavior in wireless networks". International Conference on Dependable Systems and Networks (DSN'03), San Francisco, California.

Luo, H. and S. Lu (2002) "Ubiquitous and robust authentication services for ad hoc wireless networks", UCLA Computer Science Department.

Michiardi, P. and R. Molva (2004) "Ad hoc networks security". Mobile ad hoc networking. **(1)**: 275–297.

Patwardhan, A., F. Perich (2006) "Querying in packs: Trustworthy data management in ad hoc networks." International Journal of Wireless Information Networks 13 (**4**): 263-274.

Perich, F., A. Joshi (2006) "Data Management for Mobile Ad-Hoc Networks." Enabling Technologies for Wireless E-Business: 132-176.

Ping, Y., Y. Yan, (2004) "Securing ad hoc networks through mobile agent". 3rd international conference on Information security, New York, USA, ACM.

Shaikh, R. A. and Z. A. Shaikh (2007) "A Security Architecture for Multihop Mobile Ad hoc Networks With Mobile Agents". 9th International Multitopic Conference, IEEE INMIC 2005 Karachi, Pakistan, IEEE.

Sun Microsystems (2001) "Jini Technology Core Platform Specification, version 1.2".

Xu, B. and O. Wolfson (2005) "Data management in mobile peer-to-peer networks." Databases, Information Systems, and Peer-to-Peer Computing: 1-15.

Zhang, Y. and W. Lee (2000) "Intrusion detection in wireless ad-hoc networks". 6th annual international conference on Mobile computing and networking, New York.

Zhang, Y., W. Lee, (2003) "Intrusion detection techniques for mobile wireless networks." Wireless Networks 9 (**5**): 545-556.

Zhou, L. and Z. J. Haas (2002) "Securing ad hoc networks." Network, IEEE 13 (**6**): 24-30.

Zink, M., K. Suh, (2008) "Watch global, cache local: YouTube network traffic at a campus network-measurements and implications." Proceeding of the 15th SPIE/ACM Multimedia Computing and Networking (MMCN'08).