IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. III (Sep. - Oct. 2016), PP 71-79
www.iosrjournals.org

Cryptographic Approach of Generic Caching strategy for Opportunistic Wireless Networks (OPPNETS)

L. Jai Vinita[1]
[1]*Assistant Professor, Computer science and Engineering, VNRVJIET, Hyderabad, India*

Abstract: *In Opportunistic networks, if a mobile finds that the content of its interest is available in other mobiles, it will send a message to request for the content and download it. The term subscriber denotes a node which requests for the content and the term publisher denotes a node which has the content. There can be two types of caches in a mobile node, namely private and public caches. Private cache stores the data of its own interest where as public cache stores the data of other nodes' interests. While a subscriber node requests another node for a particular content that is in the communication range for which it is missing, thereafter it forwards the request to other neighbouring nodes. In the case of public cache, there may be an intruder who issues false requests on behalf of a subscriber thereafter may get the access of the publisher's device and tries to keep the device busy always and unavailable. Thus it achieves the denial of service (DOS) attack. In this paper I investigate the various attacks that aim to degrade the public caching capabilities and propose a special kind of caching scheme called a* ***Signature Generic Cache*** *which stores the public data contents with the digital signature. Here digital signature is formed by taking the hash of the data content and then encrypting the data one by one with the publisher's private key whose purpose is to guarantee the integrity of the cached content. In one-way authentication, the publisher assures that the request is from the trusted user by validating the requester's digital certificate and thus it avoids security vulnerabilities. In order to conduct my study, I evaluate the performance of Signature generic caching scheme by using OMNET++ simulator. In this paper, I present the results by adopting the latest version of INET framework to implement the concept of Oppnets and NETA framework in order to show the various network attacks which are built on the top of OMNET++.*

Keywords: *Opportunistic Networks (Oppnets), Caching, Publisher/Subscriber, Public key Cryptography, Digital signatures, Pseudonyms, Digital certificates*

I. Introduction

Today, the mobile devices are used for two main purposes; firstly they are for voice communication as well as for data transmission. It enables users to watch videos, surf websites, etc. Specifically, data traffic from various mobile social networking (MSN) sites and mobile applications such as Facebook, Twitter, Whatsapp or Flickr tends to exceed its limit than the voice traffic. From anywhere at any time mobile users can post and share their interests through status messages and photos from their mobiles. During 2009 with reference to [2], 4.6 billion mobile subscriptions generate less voice traffic than data traffic from 400 million mobile subscriptions. There will be a doubled annual increase as reported by the forecast for the next five years. It is required to expand the network infrastructure in order to satisfy their users' demand, thus it leads the mobile operators to invest more. To support a demanding need of customers by expanding the network continuously is not an appropriate way because the operators have to purchase more hardware equipment to provide enough resources every year and the contribution cost is expensive. Moreover, in order to expand the existing network it takes longer time for the network operators. They have to forecast and plan how many devices or base stations that they have to purchase. Then, they make an order and wait until the devices are delivered. Then, the installation phase starts and thus it runs out of time until it is completely done. In addition, it consumes time to configure and test devices before launching them in the real network in order to assure that the newly-installed devices run stably and do not cause a problem to the real network. Thus there the concept of ad-hoc networks come into existence. An ad-hoc network is a wireless network without centralized infrastructure such as access points or base stations. A wireless device in the ad-hoc network establishes one-to-one connection directly with another device that is in communication range. The ad hoc network takes the benefits of decentralized server-base model. It enables users to establish a connection where the network is temporarily established or when it frequently changes. For example if a group meeting has to be arranged immediately for a short time, the network needs to be set up instantly for the moment for the users. Moreover, some users may come to the meeting late or some may leave early; accordingly, there will be a change in the network topology. In Peer to Peer network there is no need for an infrastructure and a centralized server, it obviously supports the mobility of users. Furthermore, high reliability and scalability is supported and single node failure is avoided [3]. More importantly, most models of the mobile devices available in the market nowadays can be implemented because they support various forms of radio communications in particular Bluetooth and IEEE 802.11. In the previous work [29] we introduced an adaptive reputation system for various caching schemes [26] proposed for mobile ad-hoc networks. Caching Techniques like CachePath and CacheData can significantly improve the system performance but still that is not enough for ad-hoc networks. Both of the schemes can reduce the average

number of hops between the requester and the node that has the cached data. Hybrid caching adjusts itself to the ad-hoc network environment to provide best cache performance by taking the advantage of CacheData and CachePath while avoiding their weaknesses. Regardless, some types of ad hoc networks as mentioned in [4] and [5] are based on a network overlay which is considered as virtual links. The overlay must be set up and it requires a routing protocol such as Adaptive Distance Vector routing protocol (ADV), Ad hoc On-demand Distance Vector routing protocol (AODV), etc. Data can be transmitted only when a source node and a destination node are active at the same time. This restriction is not suitable for the scenario that users frequently and unpredictably join and leave the network. In this case, it may fail to update the overlay. As a result, a message might not be delivered. Thus, the latest trend of mobile ad-hoc networking paradigm known as opportunistic wireless networks (Oppnets) becoming popular. In my previous work [32] I emphasized data on Vehicular ad-hoc Networks (VANETS) with privacy and security which is a kind of Oppnets. This paper is structured as follows: first, detailed explanation of the opportunistic wireless networks is presented. Subsequently, the proposed caching scenario is depicted. Next, the system design and the results of the simulations are shown and discussed and then follows the evaluation analysis. I conclude the paper with conclusions and future work.

II. Opportunistic Wireless Networks

The Opportunistic wireless networks do not aim to establish an end-to-end path but they make use of the availability of individual devices [6], [7]. There is no assumption about a complete path from one node to another node. Nodes that are in contact range establish direct communication via radio interfaces [8]. After they finish establishing the connection, they start exchanging data. Oppnet is a kind of Delay Tolerant Networks (DTNs). DTNs have been widespread used in various scenarios, such as wildlife tracking, vehicular network, etc. If a node finds that the content of its interest is available at its peer, it will send a message to request the content and download it from the peer. We define the term "subscriber node" for the node that requests content. The opportunistic wireless networks do not require the subscriber node and the node that has the content to be active at the same time. Both of them might never see each other at all. If the subscriber node is not currently available, a node that has the content will send it to another neighbouring node. This function is called "store-carry-forward". It will store and carry contents and may forward them if it meets a subscriber node in the future. It is also possible that the content may be disseminated to the subscriber node over multiple discontinuous wireless contacts but each one is only based on direct communication. Figure 1.1 shows the forwarding of data from node 4 to node 2 over a period of time without continuous end-to-end connectivity.

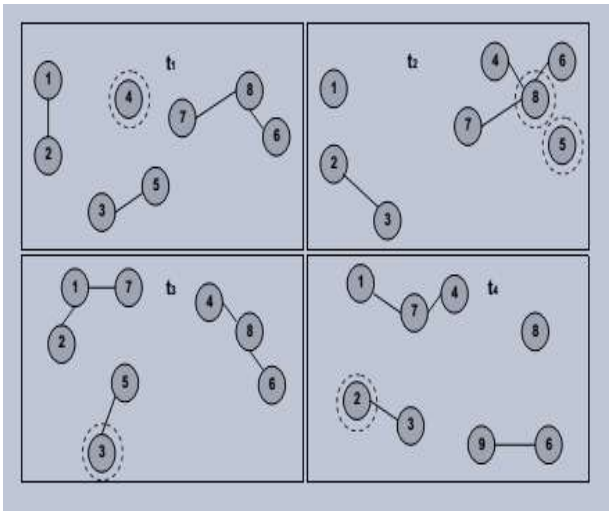

Figure 1: *Data forwarding in Oppnets*

Figure 1.2 shows a scenario of wireless opportunistic network. [30]Cindy subscribes to the song "symphony no. 12", but this content is not available in her device now. Bob who works in the same office as Cindy knows that Cindy wants this song; therefore, Bob also helps Cindy search for this song. In the morning of the next day, while Bob is taking a bus to go to work, Bob's device discovers that Alice, who took in the same bus as him, is sharing many songs. One of them is "symphony no. 12". When Bob found it, he sent a request to Alice for downloading this song from Alice and finally the song was stored in Bob's device. Then, when Bob arrived at his office, Bob met Cindy and he uploaded the song to Cindy. Eventually, Cindy got the song she wanted with Bob's assistance. This example clearly shows that the song is delivered from Alice to Cindy via Bob. Alice and Cindy never know each other and are not active at the same time. The song is transferred from Alice in the morning (7:55 A.M.) but Cindy gets it in the afternoon (12:31 P.M.).

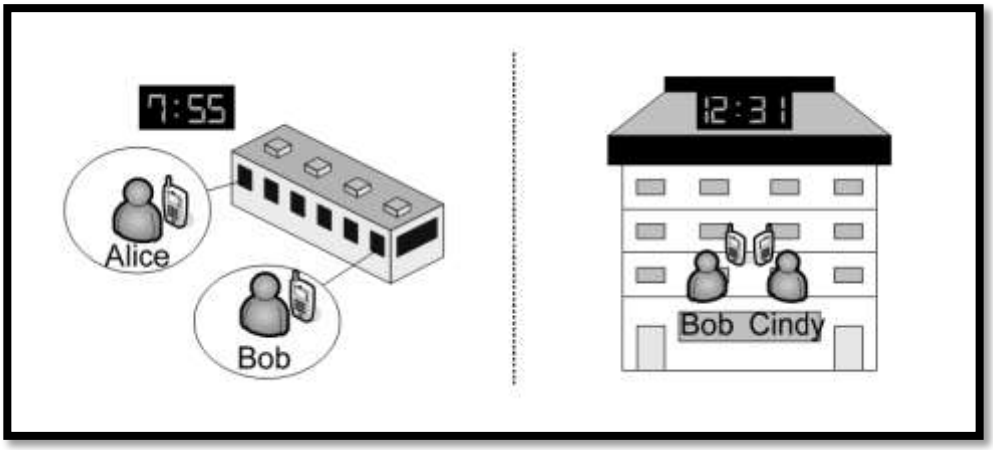

Figure 2: *A Scenario for Oppnets*

Consider the following scenario which also explains the concept of Oppnets. At a computer science conference site, researchers from all around the world stay together for 2 – 3 days to discuss recent advances in their fields. Due to the limited time, each attendee tries to make his stay as beneficial as possible, for example, by talking to colleagues during coffee breaks. For novices in research there might be the question "Who should I talk to?" or "Which other attendees are working on similar research problems?" By carrying a Bluetooth enabled mobile phone, the device is able to communicate with nearby devices carried by others in order to look for interesting conversational partners. Let's consider researchers have set their mobile phone names as research interests. Once the devices have discovered a match in research interests, the devices notify their owners and the owners are able to switch to a face-to-face communication due to the short communication range. The devices might also exchange information, for example, paper reading lists, without user notification. By this, each attendee would learn about what other researchers are currently working on. After the conference is over, this information is carried back home and the attendee might share this information with colleagues at his research institute, again, by using his mobile phone and without notice.

The Opportunistic network is a network of wireless connected nodes. Nodes may be either mobile or fixed. Communication range between two connected nodes is within walking distance, that is, 100–300 meters. The network topology may change due to node mobility or node activation and node deactivation. The nodes provide two functionalities. They are Node Discovery and One–Hop Message Exchange. Node Discovery is a network node which is able to discover other network nodes in direct communication range. One-hop Message Exchange is a node which is able to send and receive arbitrary data in form of a message to or from any other node in direct communication range. An opportunistic network node consists of a device with short-range wireless communication capabilities. The device operates an opportunistic network application that uses a data sharing protocol for data dissemination. The data sharing protocol uses node discovery and one-hop message exchange. There are two types of opportunistic network nodes. They are mobile nodes and Information Sprinklers. A mobile node consists of a user carrying a mobile device that acts as an opportunistic network node. An Information Sprinkler (IS) is a fixed opportunistic network node within the network. It is a device placed at a dedicated location, thus it is not mobile and not under direct user control. Table 1.1 depicts the comparison between Infra- structured wireless networks, Mobile ad-hoc networks and Opportunistic networks.

There are number of applications in the field of opportunistic networks [14]. For example, users can opportunistically initiate a local quiz or a poll. When a user starts up with a new quiz instance it creates a feed and publishes the quiz as the first entry. Participants subscribe to the feed and publish their answers as new entries on the feed. Information on available quizzes could also be distributed on a dedicated discovery feed.

Table 1: *Comparison between various Wireless Networks*

Type of the Network	**Layer**	**Routing**	**Node Mobility**	**Size of the Network**	**Data Forwarding**	**Node Relationship**
Infra-structured Wireless	Application	Yes	No	High	Yes	Low
Mobile Ad-hoc	Network	Yes	Yes	Medium	Yes	High
Opportunistic	Application	No	Yes	Low	Yes	Low

When participants come into communication range they exchange published entries and locally update their results. In the simplest scenario where no result aggregation is needed, each user can receive the answers from other participants and then, based on higher level logic, create its own representation of the quiz results. Another example is Social networking. Many of the current social applications that are popular on the Internet (such as Facebook or Twitter) lend themselves well to publish and subscribe and can be extended into the opportunistic domain. Each user

has a feed that followers subscribe to. Status updates, blogs or media files can be published as entries by the user. The actual data to be shared in each entry will be specified in the enclosure field, and users could for example define different feeds for separating content, e.g. an audio feed, a video feed etc. Applications falling into the social networking category are not expected to have any spatial limitations, thus the content can be spread opportunistically as long as there is interest in it. One more example is Relaying sensor data. This category relates to applications that require transporting sensor data from devices in the field to a sink node or infrastructure network. Nodes that participate in the relaying of data subscribe to feeds that the sensors publish data on.

There are two types of caching according to [30] private cache and public cache. The private cache contains only the contents that are of user's private interest, while the public cache consists of data that can be of neighbor's interest. Contents are served from both caches in a mobile device. Unfortunately, there are many threats to public caching.

Threat#1: Unauthorized information disclosure via cached data

Threat#2: Chances of escalation privilege attacks and user impersonation through cached content IDs.

Threat#3: Degrades the caching service by polluting the cache [31] with unpopular content and number of unwanted requests.

In this paper we propose a special kind of caching called ***Signature Generic cache*** which is to address aforementioned challenges. The aim is to review various caching strategies and evaluate performance of data dissemination and overhead experienced by the system as well as the vulnerabilities due to the public caching. The area in privacy and security of caching data in opportunistic networking is quite new and the existing work in this area is rare.

III. Proposed Caching Strategy

In general, users subscribe to all types of contents that they are interested in. It is possible that only some contents of interest are available in their device while some are missing. Therefore, the users (or nodes) will ask to download these missing contents from other nodes in the network. Nonetheless, all users do not have the same interests; their subscriptions vary. Therefore, when a node contacts another node that is in communication range and asks for the missing contents, there is no guarantee that the other node can upload the missing contents because the node that receives the request can share only the contents it carries, which are generally the private contents. Although the node that received the request cannot promptly provide those contents, it will try to fetch them from its neighbours to support the node that sends the request if they meet again in the future. Since these contents are not the contents of its interest, the node will store them in a public cache. Therefore, nodes may tend to follow the public caching strategies for enhancing the performance of data dissemination. As the name 'public cache' implies that it is available to all other nodes without any restrictions. The main threat to public caching is that any unauthorized malicious node floods the small network with the number of requests to the publisher and tries to exploit its quality of service. In order to overcome this problem, I propose a new additional feature to the current caching strategy called *Signature Generic cache*. Here generic cache represents public cache. Subscriber side includes the node that initiates the request and also the neighbouring nodes that forward it. From the scenario mentioned in Figure1.2 Cindy is the subscriber node, Bob is the neighbouring node and Alice is the publisher node. According to this scenario as Bob is unknown to Alice, she checks for the authenticity of Bob before it provides access to download the contents from the Generic cache.

Some possible attacks by a malicious mobile node

1. Bob could claim to be Alice to get messages intended for Alice.
2. Bob could claim that Alice is at her location so that traffic intended for Alice is sent to her (hijacking).
3. Bob could claim that Alice is at a non-existing location so that traffic intended for Alice is lost.

We could stop these attacks by ensuring that the neighbouring node who forwards the request on behalf of a subscriber is not an intruder.

A. Cryptographic Approach

Nodes contact a certificate authority (CA) that generates certificate and a public/private key pair (PR_i/PU_i). As per the above mentioned Oppnet scenario, Private Key of a node is known only to him and Public Key of a node is known only to the nodes that belong to the particular community network. The certification process ensures that each node has only one pseudonym, and the corresponding certificate can be used to prove that this pseudonym was generated by the CA and is random. Therefore, the use of this certificate effectively prevents attacks. Confidentiality and authenticity is achieved using Encryption and Digital Signatures.

The steps followed by Alice from Figure 5

At Alice's node

1. Cryptographic hash function '*h'* is computed by passing each content say ***Data*** $\boldsymbol{d_i}$ as the input from the generic cache.
2. It is then encrypted using Alice's private key to form the digital signature '*s*' of Alice for the ***Data*** $\boldsymbol{d_i}$ at publisher's side.

When Bob requests Alice for a particular content with the corresponding data id_i, clear form of content ***Data*** d_i is again fed into the hash function to compute '*h' and* the following steps taken place

At Bob's node

1. Bob decrypts the signature's' to form 'h'' by using Alice's public key which is known only to the nodes among the community.
3. If both hash functions *h* and *h'* are matching Alice provides access to Bob.

If both *h and* h' is not matching Alice will come to know that Bob is an unauthorized neighbouring node that does not belong to the community.

To support this caching strategy, I introduce the following terms.

- Private Key (PR_P) – KeyID of the publisher which is known only to him.
- Public Key (PU_p) – KeyID of the publisher which is known to all the users present in the community group network.
- Available generic list (A_g) —the list of IDs of contents available in the generic cache.
- Missing generic list (M_g) — the list of IDs of contents missing in the generic cache that a node is expected to download on behalf of other nodes.
- Available private list (A_{pr}) — the list of IDs of contents available in the private cache.
- Missing private list (M_{pr})—the list of IDs of contents missing in the private cache that the node expects to download.
- Available set (S_a) — the list of IDs of contents available in the node.
- Interested list (I_l)—the list of IDs of contents expected to be downloaded that are missing from both the private and generic caches.
- Subscribed list (S_l) — the list of IDs of contents that the node subscribes to.
- Waiting list (W_l) — the list of IDs of contents that the node expects to download from the peer that is now in contact.
- Neighbour (N) — nodes that are in communication range.
- Indirect neighbour (IN) — nodes that are not in the communication range of subscriber nodes but provide the contents that are of interest to subscriber nodes.

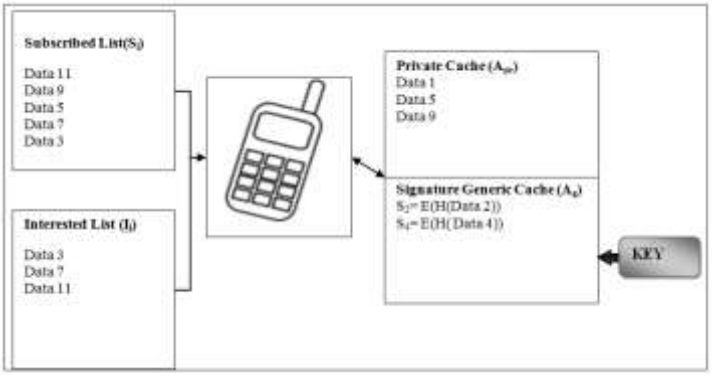

Figure 3: *Caching Model*

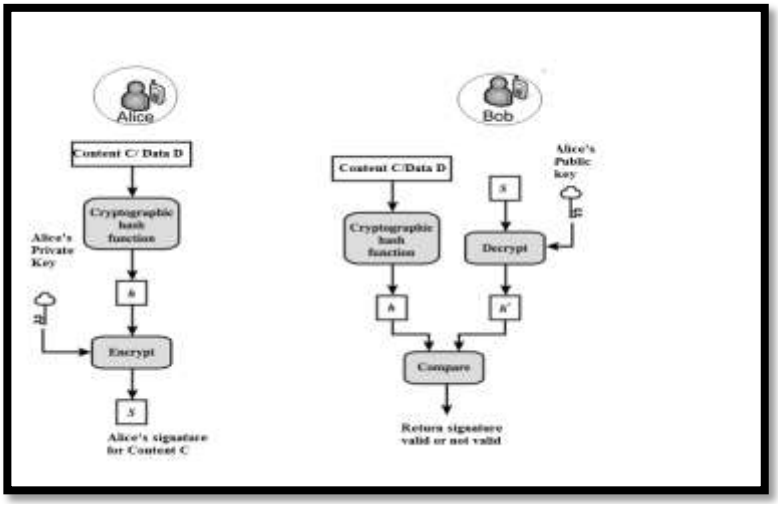

Figure 4: *Digital Signature for the Generic Cache Content*

Figure 5 shows the generation of digital signature [35] for the Content C or Data D present in the Generic cache.

B. Request Processing Algorithm

FOREACH *dataID* id_i **FROM** *GenericCache* **DO**
Compute S_i=**ENCRYPTION** (PR_p, **H(Data** d_i**))** //**Signature generation**
If *requester certificate is valid* **then**
{

Request Accepted

foreach data id_i **do**
{
If *requesteddata ID is equal to data* id_i ***then***
Compute **h = H (Data** d_i**)** // **Computation of Hashed Content**

FOREACH *Neighbouring node (N) or Indirect Neighbouring node (IN)* ***DO***
Compute **h' =DECRYPTION** (PU_p,S_i)
}
If *(h == h')* **then**
Access granted
}
Else
Request Rejected and Access denied

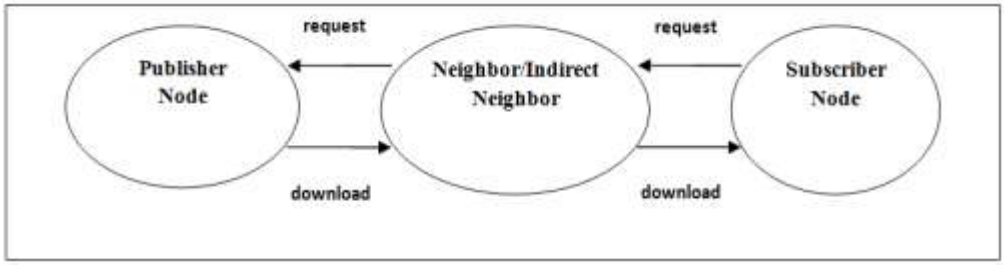

Figure 5: *Request Processing*

IV. System Design And Results

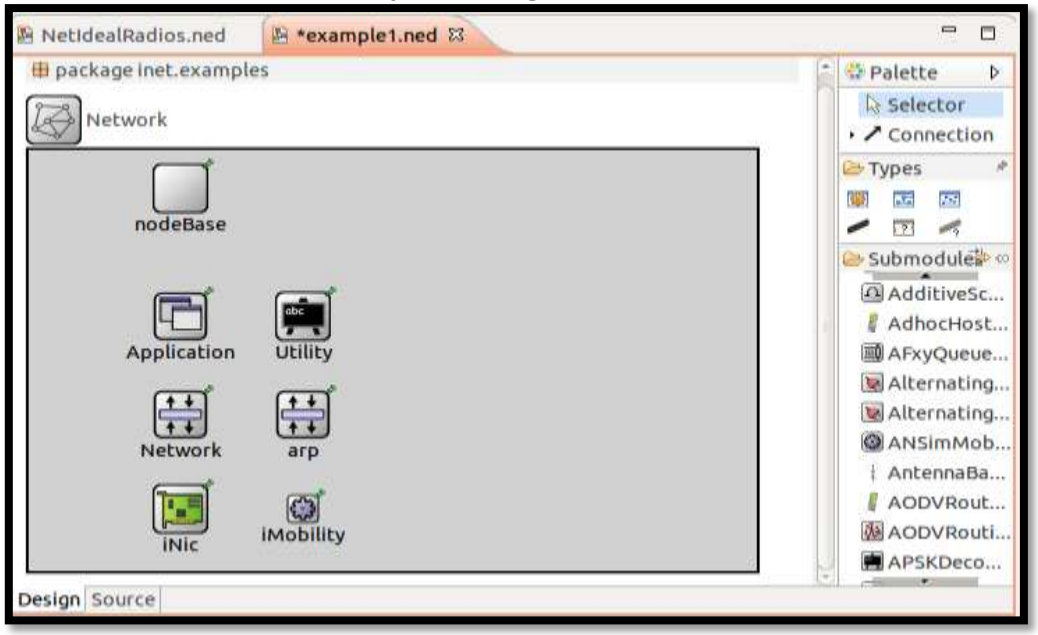

Figure 6: *Network design*

A node refers to a mobile device in the system. It carries contents, shares contents and sends messages to other nodes. Each node consists of six main modules, which are interface card (NIC) module, network module, application module, mobility module, ARP module and utility module.

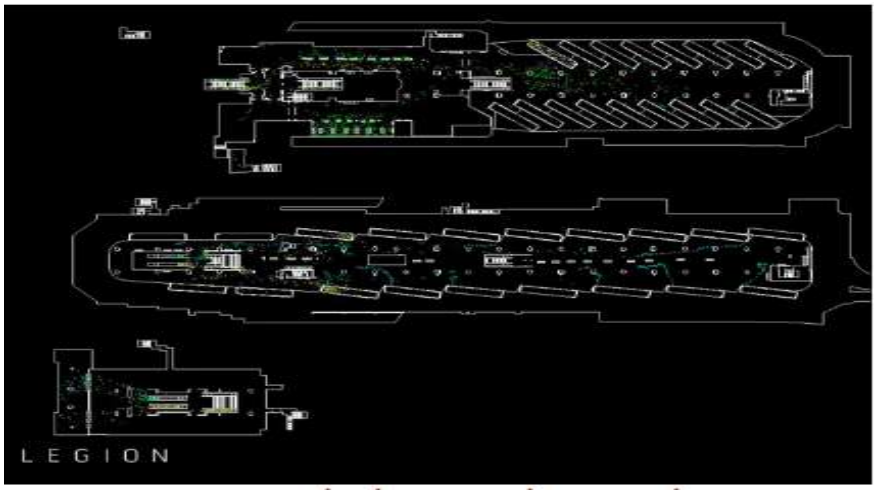

Figure 7: *Bus Terminal Pedestrian Simulations*

My simulation follows a Bus Terminal Pedestrian simulation that is created by Legion Studio which is the simulation software that simulates the behaviour of pedestrians in urban areas, subway stations, shopping malls etc.

V. Performance Analysis

In this section I evaluate the performance of my proposed system with other caching strategies without security. My proposed system deals with the authentication of the neighbouring node which sends the request to the publisher node and also the integrity of the data stored in the public cache by using public cryptographic techniques. The scheme requires asymmetric cryptography and signature computations to guarantee the local neighbourhood topology. Nevertheless, the design of the mechanism takes into account the need to minimise the number of signatures and increase its performance. The use of the pseudonym avoids signing both requests and replies, and enables the signature of requests only, thus decreasing both the computation and communication overhead: intermediate nodes have to verify and to compute only one signature each, while the initiator has to verify l_r. signatures only. Signature verification is much more efficient than signature generation. The message length is roughly the size of the three main lists Certificate list, public/private list, signature list which contain at most r + 1 element each, and in each of these elements the most important component is the public key. The message length is therefore linear in the number of hops lr. I implement the proposed Signature Generic cache strategy using OMNET++ with the frameworks INET and NETA which bring the following benefits.

- The proposed system reduces the number of inauthentic downloads.
- Publisher node verifies the certificates of the requester for the avoidance of malicious nodes.
- Digital Signatures guarantees that the data contents in the cache have not been altered by malicious nodes.
- Reduced number of malicious nodes leads to increase in network lifetime.

Table 2 *Simulation Parameters*

PARAMETERS	VALUES /RANGES
Number Of mobile nodes	10-20
Simulation area	500*500 m
Channel	Wireless channel
Mobility model	Mass Mobility
Protocol	BUBBLE-RAP
Initial Energy	100J
Data Rate	1 Mbps

VI. Conclusion And Limitations

In this paper, I proposed a cryptographic caching strategy in data dissemination for opportunistic networks by implementing public cryptographic techniques. Thus this caching strategy shows that it may decrease the number of malicious nodes which cooperate in an attempt to disturb a mobile node's service. But the limitation is that it supports only one-hop message exchange and also it supports only one way authentication. There are also restrictions in the opportunistic wireless networks. Since the subscriber node and the node that contains content items can appear in the network at any time, it cannot support real-time communication. The application which adopts opportunistic data transmission should not be sensitive to the delay.

VII. Future Work

My future work is

A. To complete the work by fulfilling the security features.
B. To include the algorithms for mutual authentication protocols that enable communicating users to verify themselves mutually about each other's identity there by exchanging session keys in a secured manner.
C. To include the algorithms in order to increase the hop limit.

References

[1]. William Stallings. *Wireless Communications and Networks*. Prentice Hall, 2005.
[2]. Ericsson. Mobile Data Traffic Surpasses Voice. Press releases. 2010, http:// www.ericsson. com/thecompany/ press /releases/ 2010/03/1396928.
[3]. Krishna Nadiminti, Marcos Dias de Assunção, and Rajkumar Buyya. *Distributed Systems and Recent Innovations: Challenges and Benefits*. Department of Computer Science and Software Engineering, The University of Melbourne, Australia, 2006.
[4]. Rajendra V. Boppana, and Satyadeva P Konduru. *An adaptive distance vector routing algorithm for mobile, ad hoc networks*. In Proceedings of IEEE INFOCOM, Anchorage, AK, USA, 2001.
[5]. Charles E. Perkins and Elizabeth M. Royer. *Ad-hoc On-Demand Distance Vector Routing*. Second IEEE Workshop on Mobile Computer Systems and Applications, New Orleans, LA , USA , 1999.
[6]. Kaustubh S. Phanse, and Johan Nykvist. *Opportunistic wireless access networks*. In Proceedings of the 1st international conference on Access networks. 2006.
[7]. Bernhard Distl, Gergely Csucs, Sascha Trifunovic, Franck Legendre, and Carlos Anastasiades. Extending the reach of online social networks to opportunistic networks with PodNet. In Proceedings of the Second International Workshop on Mobile Opportunistic Networking. 2010.
[8]. Ólafur R. Helgason, *Opportunistic Content Distribution*. Licentiate Thesis in Telecommunications, KTH, Stockholm, 2010.
[9]. Behrouz A. Forouzan, TCP/IP Protocol Suite. McGraw-Hill. 2009.
[10]. Vincent Lenders, Gunnar Karlsson, and Martin May. *Wireless Ad Hoc Podcasting*. In Proceedings of IEEE SECON, San Diego, CA, June 2007.
[11]. Martin May, Vincent Lenders, Gunnar Karlsson, and Clemens Wacha. *Wireless opportunistic podcasting: implementation and design tradeoffs*. In Proceedings of the second ACM workshop on Challenged networks. 2007.
[12]. Matthias Grossglauser and David N. C. Tse. *Mobility increases the capacity of ad hoc wireless networks*. IEEE/ACM Transactions on Networking (TON). 2002. 48
[13]. Ólafur R. Helgason, Emre A. Yavuz, Sylvia T. Kouyoumdjieva, Ljubica Pajevic, and Gunnar Karlsson. *A mobile peer-to-peer system for opportunistic content-centric networking*. In proceedings of the second ACM SIGCOMM workshop on Networking, systems, and applications on mobile handhelds. 2010.
[14]. Martin May, Gunnar Karlsson, Ólafur R. Helgason, and Vincent Lenders. *A System Architecture for Delay-Tolerant Content Distribution*. In Proceedings of IEEE Conference on Wireless Rural and Emergency Communications (WreCom), Rome, Italy, October, 2007.
[15]. Eiko Yoneki, Pan Hui, ShuYan Chan, and Jon Crowcroft. *A Socio-Aware Overlay for Publish/Subscribe Communication in Delay Tolerant Networks*. In Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems, 2007.
[16]. Chiara Boldrini, Marco Conti, and Andrea Passarella. *ContentPlace: Social-aware Data Dissemination in Opportunistic Networks*. In Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems, 2008.
[17]. Yaozhou Ma, M. Rubaiyat Kibria, and Abbas Jamalipour. *Cache-based Content Delivery in Opportunistic Mobile Ad Hoc Networks*. Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, New Orleans, LO , 2008.
[18]. Liang Hu, Jean-Yves Le Boudec, and Milan Vojnovic. *Optimal Channel Choice for Collaborative Ad-Hoc Dissemination*. In Proceedings of IEEE Infocom, San Diego, CA, 2010.
[19]. Paolo Costa, Cecilia Mascolo, Mirco Musolesi and Gian Pietro Picco. *Socially-aware Routing for Publish-Subscribe in Delay-tolerant Mobile Ad Hoc Networks*. IEEE Journal on Selected Areas in Communications. 2008.
[20]. Pan Hui, Jon Crowcroft, and Eiko Yoneki. BUBBLE Rap: *Social-based Forwarding in Delay Tolerant Networks*. In Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing, 2008.
[21]. Ólafur R. Helgason, Sylvia T. Kouyoumdjieva and Gunnar Karlsson. *Does Mobility Matter?* In Proceedings of seventh International Conference on Wireless On-demand Network Systems and Services (WONS), 2010.

[22]. Apple. IPod. http://www.apple.com/ipod/.
[23]. **L.Jai Vinita,** S.Punitha, S.Thomson. *An Adaptive Hybrid Reputation System in Caching Data for MANETS***.** CIIT International Journal of Wireless Communication Volume 3, March 2011, Pg.No: 194-204
[24]. Sanpetch Chupisanyarote. *Content Caching in Opportunistic Wireless Networks*, School of Electrical Engineering Kungliga Tekniska Högskolan Stockholm, Sweden 14 June 2011.
[25]. Liangzhong Yin and Guohong Cao. *Supporting Cooperative Caching in Ad Hoc Networks*, Issue No.01 - January (2006 vol.5), pp: 77-89
[26]. **L. Jai Vinita**, N.V. Sailaja. *Data Oriented VANETS with Privacy and Security*. CIIT International Journal of Wireless Communication, Volume 3, No 9, June 2011
[27]. K. M. Fathima Jahanas, N.Balaji, B.Dhivya. *Timely and Secure Data Transmission in Disruption Tolerant Networks*. International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 10, October 2014
[28]. Wei Gao, Guohong Cao, Arun Iyengar, Mudhakar Srivatsa. *Cooperative Caching for Efficient Data Access in Disruption Tolerant Networks*. IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 3, MARCH 2014.
[29]. William Stallings, Cryptography *and Network Security*, Fourth edition.
[30]. Yan Gao, Leiwen Deng, Aleksandar Kuzmanovic, and Yan Chen. *Internet Cache Pollution Attacks and Countermeasures*.