Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Genetic based Semantic CBMANET

Abhishek Naranje[1], Prateek Singh[2]
[1,2]Department of CSE,SSET, SHIATS, Allahabad

Abstract: A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. The special features of MANET bring this technology great opportunity together with severe challenges [1]. In MANET nodes can directly communicate to all other nodes within the radio communication range. In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. In this paper we proposed a novel approach "Semantic Content Based MANET", in this method firstly each MANET node must learn routing and security information using semantic genetic programming and then we uses full cache method for packet transaction in MANET. OPnet network simulator was used for simulation, result was compared with Full Cache Content Based MANET.

Keywords: Manet, Genetic Programming, Content Based Manet, Semantic

I. INTRODUCTION

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a
potentially hostile environment. Although security has long been an active research topic in wireline networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack.
There are two types of MANETs: closed and open. In
a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/ rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behaviour is termed selfishness or misbehaviour. [4]

In MANET security is major concern, layer wise description is as follow [3]:

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multifence security solution that is embedded into possibly every component in the network, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats. This new design perspective is what we call resiliency-oriented security design. We envision the resiliency-oriented security solution as possessing several features.

First, [5] the solution seeks to attack a bigger problem space. It attempts not only to thwart malicious attacks, but also to cope with other network faults due to node misconfiguration, extreme network overload, or operational failures. In some sense, all such faults, whether incurred by attacks or misconfigurations, share some common symptoms from both the network and end-user perspectives, and should be handled by the system.

Second, [6] resiliency-oriented design takes a paradigm shift from conventional intrusion prevention to intrusion tolerance. In a sense, certain degrees of intrusions or compromised/captured nodes are the reality to face, not the problem to get rid of, in MANET security. The overall system has to be robust against the breakdown of any individual fence, and its performance does not critically depend on a single fence. Even though attackers intrude through an individual fence, the system still functions, but possibly with graceful performance degradation. Third, as far as the solution space is concerned, cryptography-based techniques just offer a subset of toolkits in a resiliency-oriented design. The solution also uses other non crypto-based schemes to ensure resiliency. For example, it may piggyback more “protocol invariant” information in the protocol messages, so that all nodes participating in the message exchanges can verify such information.

As discussed in [7] system may also exploit the rich connectivity of the network topology to detect inconsistency of the protocol operations. In many cases, routing messages are typically propagated through multiple paths and redundant copies of such messages can be used by downstream nodes. Fourth, the solution should be able to handle unexpected faults to some extent. One possible approach worth exploring is to strengthen the correct operation mode of the network by enhancing more redundancy at the protocol and system levels. At each step of the protocol operation, the design makes sure what it has done is completely along the right track. Anything deviating from valid operations is treated with caution. Whenever an inconsistent operation is detected, the system can raise a suspicion flag and query the identified source for further verification. This way, the

protocol tells right from wrong because it knows right with higher confidence, not necessarily knowing what is exactly wrong. The design strengthens the correct operations and may handle even unanticipated threats in runtime operations.

Next, the solution given in [8] may also take a collaborative security approach, which relies on multiple nodes in a MANET to provide any security primitives. Therefore, no single node is fully trusted. Instead, only a group of nodes will be trusted collectively. The group of nodes can be nodes in a local network neighbourhood or all nodes along the forwarding path. Finally, the solution relies on multiple fences, spanning different devices, different layers in the protocol stack, and different solution techniques, to
guard the entire system. Each fence has all functional elements of prevention, detection/verification, and reaction. The above mentioned resiliency-oriented MANET security solution poses grand yet exciting research challenges. How to build an efficient fence that accommodates each device's resource constraint poses an interesting challenge.

II. LITERATURE SURVEY

Researchers has done lots of concrete efforts in the field of MANET security one of the most appreciate work was carried by Leovigildo Sanchez-Casado, Rafael A. Rodrguez-Gomez, Roberto Magan-Carrion, and Gabriel Macia-FernandezLeovigildo Sanchez-Casado, Rafael A. Rodrguez-Gomez, Roberto Magan-Carrion, and Gabriel Macia-Fernandez in the development of NETA[3] Evaluating the effects of NETwork Attacks. They have built NETA as an OMNeT++[20] simulator framework built on top of the INET framework. NETA is intended to be widely used by the research community, considering that OMNeT++ is one of the most common simulation tools in the networking. Additionally, NETA framework is based on the same idea as OMNeT++, i.e., modules that communicate by message passing.

MANET security was very closely analysis and addressed by HAO YANG in [4], as Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both proactive and reactive approaches, and encompass all three components: prevention, detection, and reaction.

K.Kirubani, S.P.Anbukodi has done a remarkable research [5] as MANET doesn't need a set of network infrastructure; each single node works as each a transmitter and a receiver and they trust their neighbors to relay messages. Nodes communication directly with one another once they are in range intervals constant communication varies. The self-configuring ability of nodes in MANET created it fashionable among vital mission applications like military use or emergency recovery. Unfortunately, the open medium and remote distribution of MANET create it at risk of numerous kinds of attacks. So, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. MANET into industrial applications. In this project, we define solid privacy requirements regarding malicious attackers in MANET. Then we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

Prof. Sachin Lalar of TERI proposed following method [6] for MANET security. Here multi-layer intrusion detection technique is a technique in which an attacker attacks at multiple layers in order to stay below the detection threshold so that they will escape easily whenever a single layer impropriety detects. These type of attacks mainly attack at cross layer which are more alarming and frightening as compare to single layer attack and they can easily be escaped. Although these type of attacks can be detected by a multiple layer insubordination detector, where with respect to all network layer's input are use to combine and examine by the cross-layer detector in a detailed fashion. There is also another way to detect these kinds of attacks by working together with RTS/CTS and network layer detection with respect to dropped packets.

Another significant work was done by using Content Based coding MANET [2] we studied the fundamental of Content Based MANET as follow:
In content-based networks, addressing shifts from host based addressing to content-based addressing. Each transmission unit (content block) is uniquely identified. In dynamic, intermittent networks bandwidth is scarce. However, storage is becoming increasingly cheaper. The trend of increasingly cheap storage suggests to embrace the delay tolerant network philosophy of compensating for intermittent connectivity with intermediate node caches. In case of popular files, this allows requestors to download from multiple caches even when the origin is unreachable. In intermittent networks, the following challenges affect file dissemination:
• Last coupon problem: Teams may form and split frequently, thus a file must be transmitted (and can be
retrieved from caches) in a piecemeal fashion. Thus,
pieces are received out of order. This makes it difficult
for the requestor to reliably reconstruct a file.
• Partial caches: Various nodes contain different parts
of a file.
• Busy caches: A requestor may find out that a cache
which has the required pieces is busy serving other
requestors. This causes the requestor to either wait
for the next transmission opportunity or locate another
Cache. Content coding can help address each of the above challenges. In particular:
• Last Coupon Problem: By using content coding, the
last coupon problem is eliminated since with high probability any coded block received is innovative (i.e., helpful) and can be used to reconstruct the file.
• Intermittent Connectivity: In case of intermittence, locks are cached at intermediate nodes. A requestor
Periodically sends out interests and retrieves the blocks
from nearby caches.
• Parallel Cache Download: When a requestor finds a
nearby cache busy to answer requests, it can ask other
nearby caches for blocks since each network coded
block is as helpful as any other.

And to understand semantic coding approach we learn fundamental semantic concepts from Semantic Search-Based Genetic Programming and the Effect of Intron Deletion [8] as follow:
The idea consists in building, maintaining, and updating generation by generation a semantically distribution, biasing the search toward areas of the semantic space characterized by good fitness values. Fundamentally a distribution of size and biases the search toward sizes associated with good fitness values, among the ones evolved so far. The similarities between Semantic- Genetic Programming and OpEq, however, are limited to the acceptance criteria of new individuals produced by the genetic operators. Beyond this, the basic idea that characterizes the two methods is different: While OpEq builds and uses a distribution based on the syntax of the individuals, the study proposed here focuses on semantics. For experimental implementation we consider a set of well-known noncontinuous test functions, comparing the performances of SEM- Genetic Programming with the ones of standard Genetic Programming and a well-known Genetic Programming variant called bacterial Genetic Programming, which was introduced in [9]. Both Standard- Genetic Programming and Bacterial- Genetic Programming use genetic operators that are completely based on the solutions syntax. Besides studying the effect of Semantic-Genetic Programming on the quality of the generated solutions (in terms of fitness).

III. PROPOSED METHOD

A Semantic Approach to coding in Content Based MANETs

Our proposed solution is "A semantic approach Content Based -MANET", where Semantic – Genetic Programming will use to improve the performance of fully cache Content Based MANET, which will use semantic search based Genetic Programming and creates meaning fully understanding among the all the nodes (Source as well as intermediate) this will improves the performance of system drastically.

3.1 Preliminary concepts:

In content-based mobile ad hoc networks (Content Based MANETs), random linear network coding can be used to reliably disseminate large files under intermittent connectivity. Conventional Network Coding involves random unrestricted coding at intermediate nodes. This however is vulnerable to pollution attacks. To avoid attacks, a brute force approach is to allow mixing only at the source. However, source restricted Network Coding generally reduces the robustness of the code in the face of errors, losses and mobility induced intermittence. Content Based -MANETs introduce a new option. Caching is common in Content Based MANETs and a fully reassembled cached file can be viewed as a new source. Thus, Network Coding packets can be mixed at all sources (including the originator and the intermediate caches) yet still providing protection from pollution. The hypothesis we wish to test in this paper is whether in Content Based MANETs with replicated caches of a file, the performance (in terms of robustness) of the coding restricted to full caches equals that of unrestricted coding.

3.2 SEMANTIC- Genetic Programming: The Algorithm

In the beginning of the evolutionary search, a new semantic niche sni is created for every program pi of the initial population. Each sni is represented by the same vector wsni that represents the semantics wpi of pi . In order to enforce semantic diversity, it is required that no semantically similar individuals are generated during the initialization process. For this purpose, an iterative process is implemented that discards every newly created individual if it is found to be semantically similar to one of the already generated programs. As discussed earlier, semantic similarity is governed by a threshold value on the average Canberra distance between two semantic vectors wp1 and wp2 ,
where p1 and p2 are their respective programs. The process iterates as many times as necessary to create the initial population, in light of offspring rejections that take place in the attempt to enforce semantic diversity. At the end of the initialization process, each semantic niche has a capacity equal to one. Semantic- Genetic Programming uses a generational replacement strategy by which an intermediate population is created through the application of variation operators, and at the end of this process the intermediate population replaces the current population. The creation of an intermediate population is described in the pseudocode of Algorithm 1. The main constituent elements are as follows.

1) A procedure that updates the semantic distribution by reallocating individuals in semantic niches and calculating the capacities for the next generation (depicted in Algorithm 3).

2) A procedure that handles an offspring's acceptance in the intermediate population, forcing the sampling of new programs to be governed by the semantic distribution (depicted in Algorithm 2).

Algorithm 1 Creation of an Intermediate Population

```
update_semantic_distribution();
N_accepted :=0;
While n_accepted <  pop_size do
        Select parents from population;
        apply variation operator;
        for (every offspring p) do
            if(acceptance_criterion(p))
```



```
            then
                    insert p in the new population;
                    n_accepted=n_accepted + 1;
            fi
        od
    od
```

Algorithm 2 Offspring Acceptance Criterion

```
Proc Boolean acceptance_criterion (program p)
  W_p:= extract program p semantics;
   If (semantic_similarity(w_p)
       then
         w_closest:=get_closest_niche(w_p);
         if(size(w_closest)≥ capacity(w_closest))
             then
                 if(p is the best of w_closest)
                     then
                         size(w_closest):=size(w_closest)+1;
                         return:= true;
                      else
                           return := false;
                    fi
            else
                  size(w_closest):=size(w_closest)+1;
                  return:= true;
                     fi
              else if (p is the best of the run)
                  then
                          create new niche w_p;
                          return := true;
                  else
                          return := false;
                    fi
           else
                  return:= false;
    fi
end
```

Algorithm 3 Semantic Distribition Update

```
Proc void update_semantic_distribution()
  If( a new niche has been created)
     Then
         for(every program p in population) do
            w_p:=extract program p semantics;
            w_closest := get_closest_niche(w_p);
```


allocate p into niche represented by $w_{closest}$;
od
else
fi
for(every niche i) do

$$\text{capacity(i)}:=\left[\left(1-\frac{\bar{e}_{sn_i}}{\sum_{i-1}^{n} e_{sn_i}}\right)*\text{pop\_size}\right]$$

size(i):=0;
od
end

Algorithm 4 Deretmination of the closest Semantic Niche

Proc semantics get_closest_niche(semantics w)
D:={};
for (every exiting niche i) do
d(w, w_{sni}):=0
for(j=1 to length(w)) do

$$d\left(w, w_{sn_i}\right)=d\left(w, w_{sn_i}\right)+\frac{abs(w[j]-w_{sn_i}[j])}{abs(w[j]+abs\, w_{sn_i}[j])}$$

od

$$d\left(w, w_{sn_i}\right)=\frac{d\left(w, w_{sn_i}\right)}{length(w)}$$

$$D:=D\cup d\left(w, w_{sn_i}\right)$$

od
return w_i for which d(w,w_i) is smallest in D
end

Algorithm 4 Determination of Semantic Similarity

proc boolean semantic_similarity(semantics w)
$w_{closest}$:= get_closest_niche(w_p);
if(d (w, $w_{closest}$) <semantic_similarity_threshold)
then
return true;
else
return false;
fi
end

3.3 Semantic CONTENT BASED MANET Procedure:

1) Using algorithm 1 to 5, all the mobile nodes of MANET will get semantic framework.
2) AODV routing algorithm will use for routing the packet in the network.
3) Full cache Content Based MANET implementation.
4) Transaction of large files among the mobile node in secure environment.

4. SIMULATION AND RESULT:

Simulation of semantic CB MANET was completed using OPNet [21]. (Optimized Network Engineering Tools) is a discrete-event network simulator first proposed by MIT in 1986. It is a well-established and professional commercial suite for network simulation. It is actually the most widely used commercial simulation environment. OPNET Modeler features an interactive development

environment allowing the design and study of networks, devices, protocols, and applications. For this, extensive lists of protocols are supported. Network topologies are as follow:

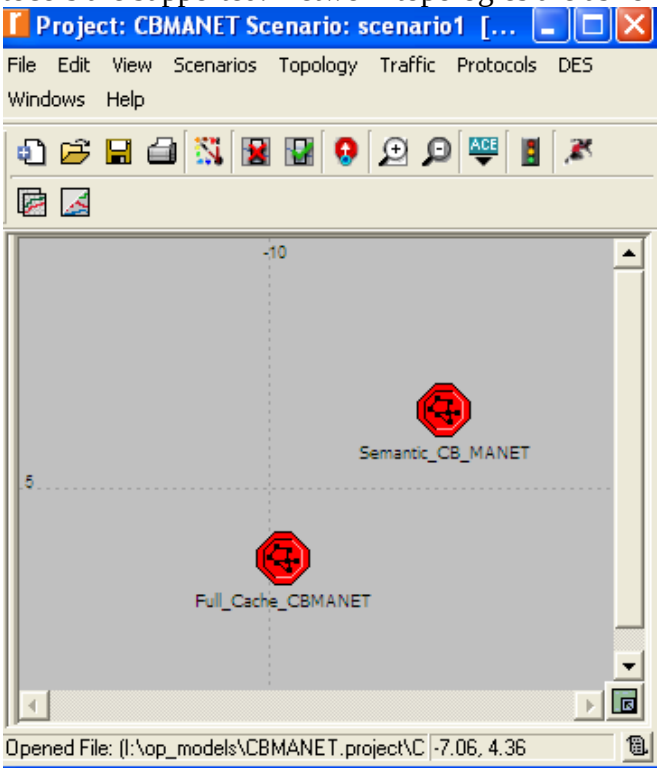

Fig. 1 Snapshot of Semantic & Full Cache CB MANET subnets

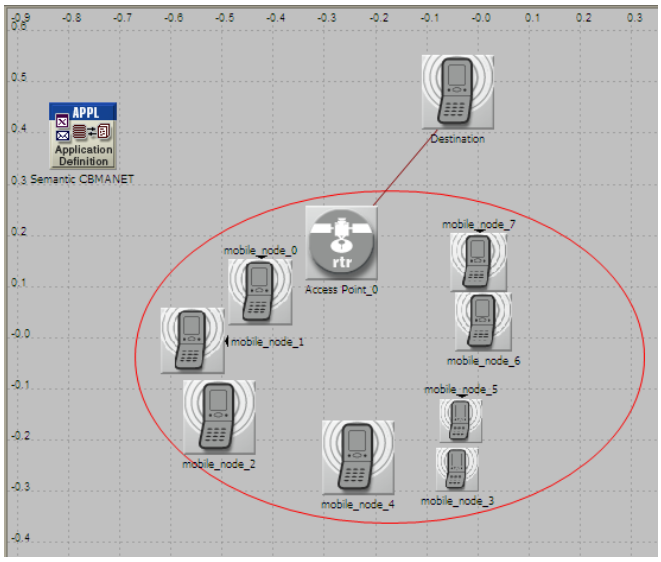

Fig. 2 Snapshot of Semantic Content Based MANET from OPNet

Fig.1, 2 represents subnets and network description diagram of semantic CB MANET respectively. In fig.1 there are two subnets semantic CB MANET subnet and full cache CB MANET subnet under the parent subnet campus.

In fig.2 we represented the network description diagram of semantic CB MANET having eight mobile units, one wireless gateway, one destination and one application configuration module (APPL).

4.1 Parameter for performance evaluation:

For performance evaluation we have used file delay rate as the parameter, which is the ratio of file delivered within delay with respect to time taken. Our result is as follow:

Table 1: Delay report comparison

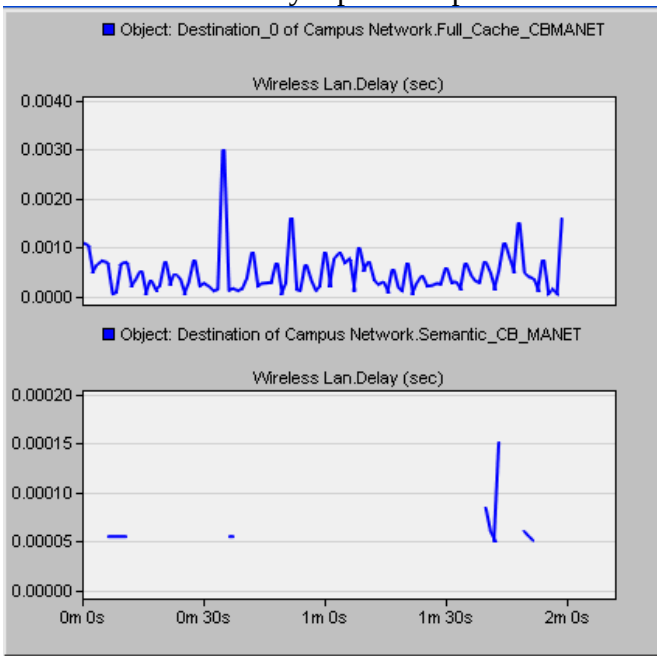

Fig. 4 File delay Rate graph

Simulation results shows that while reliable dissemination of large files under intermittent connectivity, Semantic content based MANET approach work far better than Full cache approach in terms of file delay.

V. CONCLUSION

Our solution "A semantic approach Content Based -MANET" which uses semantic search based Genetic Programming and creates meaning fully understanding among the all the nodes (Source as well as intermediate) this improves the performance of system drastically. And by simulation this was proved that semantic Content Based MANET is better and secure than Fully Cache Content Based MANET.

REFERENCES

[1] Jun-Zhao Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", IEEE 2001, pp. 316-321
[2] Joshua Joy, Yu-Ting Yu, Victor Perez, Dennis Lu, Mario Gerla, "A New Approach to Coding In Content-Based MANETs", IEEE 2014, pp. 173-177
[3] Leovigildo Sanchez-Casado, Rafael A. Rodrguez-Gomez, Roberto Magan-Carrion, and Gabriel Macia-Fernandez, "NETA: Evaluating the effects of NETwork Attacks. MANETs as a case study", Leovigildo Sanchez-Casado et al 2013, pp 01-10
[4] HAO YANG, HAIYUN LUO, FAN YE, SONGWU LU, AND LIXIA ZHANG, "SECURITY IN MOBILE AD HOC NETWORKS", IEEE Wireless Network 2004, pp. 38-47
[5] K.Kirubani, S.P.Anbukodi, "A Secure Intrusion Detection System for Manets by using Cryptographic Algorithms", IJAREEIE 2014, pp.7923-7931
[6] Sachin Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", ijmcr 2014, pp. 62-68
[7] Michael Klein Birgitta K¨onig-Ries Philipp Obreiter, "Service Rings – A Semantic Overlay for Service Discovery in Ad hoc Networks", IEEE 2003, pp. 1529-4188
[08] Mauro Castelli, Leonardo Vanneschi, and Sara Silva, "Semantic Search-Based Genetic Programming and the Effect of Intron Deletion", IEEE 2014, pp. 103-113

[09] Ekata Gupta, Dr. S. K. Saxena "A SECURITY BASED ARCHITECTURE FOR MANET", International Journal of Computing and Corporate Research, International Manuscript ID: 2249054XV4I1012014-01
[10] S.-H. Lee, M. Geria, H. Krawczyk, K.-W. Lee, and E. Quaglia, "Performance evaluation of secure network coding using homomorphic signature," in Network Coding (NetCod), 2011 International Symposium on, 2011, pp. 1--6.
[11] J. Scott, P. Hui, J. Crowcroft, and C. Diot, "Haggle: A networking architecture designed around mobile users," in WONS, 2006.
[12] J. Su, J. Scott, P. Hui, J. Crowcroft, E. De Lara, C. Diot, A. Goel, M. H. Lim, and E. Upton, "Haggle: seamless networking for mobile applications," in Proceedings of the 9th international conference on Ubiquitous computing, ser. UbiComp '07 . Beriin, Heidelberg: Springer-Verlag, 2007, pp. 391--408 . [Online]. Available: http://dl.acm. org/citation.cfm?id=1771592.1771615
[13] E. Nordstrom, P. Gunningberg, and C. Rohner, "Haggle: Relevanceaware content sharing for mobile, devices using search."
[14] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of the 5th international conference on Emerging networking experiments and technologies, ser. CoNEXT '09. New York, NY, USA: ACM, 2009, pp. 1-12. [Online]. Available: http://doi.acm.orgllO.114511658939. 1658941
[15] S. Y Oh, M. Gerla, and A. Tiwari, "Robust manet routing using adaptive path redundancy and coding," in Proceedings of the First international coriference on COMmunication Systems And NETworks, ser. COMSNETS'09. Piscataway, NJ, USA: IEEE Press,
2009, pp. 224--233. [Online]. Available: http://dl.acm.org/citation.cfm?id=1702135.1702167
[16] S. Oh and M. Geria, "Protecting network coded packets in coalition networks," in Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Coriference on, 2010, pp. 168-175.
[17] U. Lee, J.-S. Park, J. Yeh, G. Pau, and M. Geria, "Code torrent: content distribution using network coding in vanet," in Proceedings of the 1st international workshop on Decentralized resource sharing in mobile computing and networking, ser. MobiShare '06. New York, NY, USA: ACM, 2006, pp. 1-5. [Online]. Available: http://doi.acm.org/l0 .1145/1161252.1161254
[18] J.-S. Park, M. Gerla, D. Lun, Y Yi, and M. Medard, "Codecast: a network-coding-based ad hoc multicast protocol," Wireless Communications, IEEE, vol. 13, no. 5, pp. 76--81, 2006.
[19] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks,"
in Proceedings of the second ACM conference on Wireless network security. ACM, 2009, pp. 111-122.
[20] Zhongliang Zhao, and Torsten Braun**"**OMNeT++ based Opportunistic Routing Protocols Simulation: A Framework**"** in Institute of Computer Science Applied Mathematics, University of Bern Neubruckstrasse 10, 3012 Bern, Switzerland.

