Survey of secure content based MANET's

Srashti Badkul, Brajlata Chourasiya(Asst.Prof.)

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 neighbour relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics also introduce reliability problem, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors.

In this paper we have surveyed various techniques for secure MANET; CB-MANET is one of the effective methods to achieve security in MANET. In CB-MANET we can protect network from pollution attack using NC [2], and semantic programming approach can improve the performance of CB-MANET.

***Index Terms*: CB-MANET, INTRUSION, SEMANTIC, GENETIC PROGRAMMING.**

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, 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,

ISSN: 2278 – 7798

share some common symptoms from both the network and end-user perspectives, and should be handled by the system. Second, 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. The 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 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. Device heterogeneity is one important concern that has been largely neglected in the current security design process. However, multifence security protection is deployed throughout
the network, and each individual fence adopted by a single node may have different security strength due to its resource constraints. A node has to properly select security mechanisms that fit well into its own available resources, deployment cost, and other complexity concerns. The security solution should not stipulate the minimum requirement a component must have. Instead, it expects best effort from each component. The more powerful a component is, the higher degree of security or resiliency it has. Next, identifying the system principles of how to build such a new-generation of network protocols remains unexplored.

The state-of-the-art network protocols are all designed for functionality only. The protocol specification fundamentally assumes a fully trusted and well-behaved network setting for all message exchanges and protocol operations. It does not anticipate any faulty signals or ill-behaved nodes. We need to identify new principles to build the next-generation network protocols that are resilient to faults. There only exist a few piecemeal individual efforts. Finally, evaluating the multifence security design also offers new research opportunities. The effectiveness of each fence and the minimal number of fences the system has to possess to ensure some degree of security assurances should be
evaluated through a combination of analysis, simulations, and measurements in principle. However, it is recognized that the current evaluation for state-of-the-art wireless security solutions is quite ad hoc. The community still lacks effective analytical tools, particularly in a large scale wireless network setting. The multidimensional trade-offs among security strength, communication overhead, computation complexity, energy consumption, and scalability still
remain largely unexplored. Developing effective evaluation methodology and toolkits will probably
need interdisciplinary efforts from research communities working in wireless networking, mobile systems, and cryptography.

II. LITERATURE SURVEY

2.1 A Secure Intrusion Detection System for Manets by using Cryptographic Algorithms [5]: This approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. EAACK is consisted of three major components, namely, ACK, secure ACK, and misbehavior report authentication. In order to distinguish different packet varieties in different schemes, we tend to enclose a 2-b packet header in EAACK.

ISSN: 2278 – 7798

A. ACK: ACK is essentially associate end-to end acknowledgment scheme. It acts as a district of the hybrid scheme in EAACK, attending to scale back network overhead once no network misconduct is detected. In ACK mode, node S initial sends out associate ACK information packet Pad1 to the destination node D. If all the intermediate nodes on the route between nodes S and D square measure cooperative and node D with success receives Pad1, node D is needed to remand associate ACK acknowledgment packet Pak1 on a similar route however in a very reverse order. Inside a predefined fundamental quantity, if node S receives Pak1, then the packet transmission from node S to node D is winning. Otherwise, node S can switch to S-ACK mode by causing out associate S-ACK information packet to sight the misbehaving nodes within the route.

B. S-ACK: The S-ACK scheme is associate improved version of the TWOACK scheme projected by Liu et al. The principle is to let each three consecutive nodes work in a group to sight misbehaving nodes. For each three consecutive nodes within the route, the third node is needed to send associate S-ACK acknowledgment packet to the primary node. The intention of introducing S-ACK mode is to sight misbehaving nodes within the presence of receiver collision or restricted transmission power.

C. MRA: The MRA scheme is used to resolve the weakness of Watchdog once it fails to sight misbehaving nodes with the presence of false misconduct report. The false misconduct report may be generated by malicious attackers to incorrectly report innocent nodes as malicious. The core of MRA scheme is to attest whether or not the destination node has received the reported missing packet through a special route. Once the destination node receives associate MRA packet, it searches its native knowledge base and compares if the reported packet was received. Otherwise, the misconduct report is trusty and accepted. By the adoption of MRA theme, EAACK is capable of sleuthing malicious nodes despite the existence of false misbehavior report.

D. Digital Signature: As mentioned before, EAACK is associate acknowledgment based IDS. All three components of EAACK, namely, ACK, S-ACK, and MRA, square measure acknowledgment-based detection schemes. All of them believe on acknowledgment packets to sight misbehaviors within

the network. Otherwise, if the attackers square measure good enough to forge acknowledgment packets, all of three schemes will be vulnerable. With reference to this imperative concern, we tend to incorporated digital signature in our projected theme. So as to make sure the integrity of the IDS, EAACK needs all acknowledgment packets to be digitally signed before they are sent out and verified till they're accepted.

2.2 Secure Multicasting [6]: Multicast is a mechanism where any user become the part of multicast group and even send traffic to the multicast users as well as receive traffic, but due to this procedure it can easily fall into denial of service attacks (DoS). There is an architecture usually used to secure multicast traffic that is DIPLOMA. DIPLOMA stands for Distributed Policy enforcement Architecture which is use to protect or secure end user services as well as network bandwidth. Audio and video traffic usually fall into the category of multicast traffic which is usually use by militaries as well as disaster backup plans (teams). There are some of the major responsibilities of DIPLOMA architecture which are given below [Alicherry and Keromytis].

i. It gives solution for both sender and receiver whenever they access to the multicast group.
ii. It also used to limit the bandwidth.
iii. DIPLOMA integrates with common multicasting routing protocols like PIM-SM and ODMRP.
iv. It also uses to provide (allocate) network resources in a fair manner during attacks.

2.3 Secure routing: MANET is a self organized wireless network, due to the fact it has vulnerable attacks that can easily damage the whole network; that's why there should be some solutions which works even some of the mobile nodes compromised in the network. One of the primary challenges of secure routing is to provide authentication (trustworthiness) of users in the network. In case of distributed communication environment in MANET, authentication is open and any un-authentic node may be use to compromise routing traffic in order to disrupt the communication. There are some of the major responsibilities of secure routing which are given below.

i. It provides assurance that modified and replayed route replies should be rejected in order to avoid fabrication of attacks.
ii. Routing protocol responsiveness itself provide safety among different routing attacks.

2.4 Privacy-aware and Position based Routing: MANET is a kind of wireless network in which mobile nodes move from one station to another. In this type of network environment routing process among different nodes is important that's why privacy-aware and position based routing is used to avoid route overhead. In case of position based routing mechanism, a mobile node within the MANET network broadcast its position co-ordinates as well as its one-hop neighbours. This information can easily be attacked, so therefore privacy-aware mechanism is together with position based routing in order to provide secure communication. PPBR stands for privacy aware and position based routing in which a mobile node mainly takes pseudo identifiers that are usually dynamic and it is also use to provide end-to-end inconspicuousness to other nodes.

2.5 Key management: Certified Authority (CA) is one of the mechanisms which provide key management; if it

ISSN: 2278 – 7798

is compromised then entire network can easily be damaged. One of the major functionality of key management and distribution for MANET, it provide solutions for mobility related issues. In section [Biswas et al] writers discuss different aspect of key management and distribution for MANET. In the paper, the approach for key management use to solve high mobility issue as well as it provide an efficient method to reduce control overhead also gives an idea how to increase reliability in key management with respect to conventional key management process.

2.6 Intrusion detection System: Intrusion detection system is a complete security solution which provides information about malicious activities in the network, it also uses to detect and report about malicious activities. MANET is also design for route traffic mechanism when there is congestion in the network, faulty nodes as well as topology changes due to its dynamic behavior. IDS use to detect critical nodes and then analyze its data traffic, critical node also degrade network performance. There are different IDS systems which has some specific features, some of them are given blow

i. Cluster based voting
ii. Neighbour-monitoring
iii. Trust building for detail description of these IDS system sees section [Kimaya et al].

2.7 Multi-layer Intrusion detection technique: 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.

2.8 CB-MANET [8]: 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 embracing 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 fonn 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 intennittence, blocks are cached at intennediate 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.

2.8.1 FULL C ACHE CODING

In CB-MANETs, files are opportunistically cached at mobile nodes to favor future file requests. Files can be downloaded in parallel from multiple caches to make downloads reliable and fast. Network coding across parallel caches further improves the throughput. However, in intennittent connectivity, caches may often be partial. Thus, these caches cannot be signed since the signature implies that the intennediate node has received the full file, has verified the signature and has replaced in each block the originator signature with its own. Note that an intennediate cache can reconstruct the file from contributions from different caches as jn the traditional unrestricted coding. One may then state that the full cache strategy is like the unrestricted strategy in the following manner. As soon as an intennediate node decides to mix, it must fully reassemble the file and verify integrity before it reissues newly mixed packets. As we shall see, this intennediate full cache mixing can improve perfonnance significant as compared to source only coding. The above implies that the full cache strategy must be network coding aware. The question is whether a node should fully cache and decode/recode before forwarding (and signing) or should just forward the blocks as it receives them, no signature required. There is a trade off between reassembly delay (-) and improved orthogonality (ie. linear independence) of the packets (+).

2.9 Service Rings – A Semantic Overlay for Service Discovery in Ad hoc Networks:

Its an approach for semantic service discovery based on a transport-layer overlay. Overlay structure of this approach is as follow:

ISSN: 2278 – 7798

• Decentralization. The overlay structure should not be dependent on central devices (like in trees or stars) as no device could guarantee its availability in a highly dynamic ad hoc network.
• Easy and Local Adaptability to Frequent Topology Changes. Changes in the network topology should lead to repairs without great overhead and without changes in the overall overlay structure.
• Basis for Effective and Efficient Trading Mechanisms. Service trading in the overlay should avoid network flooding and always yield complete and correct answers.
• Semantic Overlay. The overlay should be able to route messages by inspecting their semantical content.
Basic Idea is a structure that fulfils these design goals are our service rings. A service ring ideally groups together devices that are both physically close to each other and offer similar services. Each ring possesses a designated service access point (SAP) which knows a summary about all services offered within its ring. SAPs can be connected to a ring, too, which leads to a hierarchical structure. Once service offers are organized this way, searching for services becomes considerably more efficient: Search messages are routed through the rings and will descend into subrings only if their SAP knows that the service might be offered within this particular subring. Thus, large parts of the network do not need to be visited at all, without having to fear that matching services might be overlooked. In the following subsections we are taking a more detailed look at these service rings.

2.10 Semantic Search-Based Genetic Programming and the Effect of Intron Deletion:
The main idea of the "semantic niching" method is to use a semantic distribution to guide the evolutionary process. This distribution is used to direct the algorithm toward solutions that are semantically close to the best solution found so far by GP. Some preliminary concepts is although there is no firm consensus around the formalization of this term, we may roughly define the expression semantics as a concise and minimal (irreducible) description of what the program is doing, expressed in simpler terms than
the original GP tree (for the sake of this study, we identify a GP program with a tree). As GP programs usually process some input data, semantics is often defined with respect to them.
2.11 A SECURITY BASED ARCHITECTURE FOR MANET [9]: In this architecture of cooperative security agents we pass DRI and ST-RT table as an input to Cooperative Security Agents. Monitor processing takes charge of monitoring all one-hop neighbours' activities and filtering and encoding them. In the Memory Library, the behavior patterns of attack nodes are kept to represent various known attack methods. Mode 1: Rec (N1, M), Delete (N1, M). Node N1 receives the message M and then deletes it, not transmitting it in accordance with the routing table. It is Interrupt Attack. Mode 2: Rec (N1, M), Modify(S N1, M), Send (N1, M). Node N1 receives the message M, and then transmitting it to next hop node after modifying packet content. Next hop node will receive the wrong packet information. It is the Error Message Attack. Mode 3: Rec (N1, M), Reply (M, N), Send (N1, N). Node N1 receives message M, and then sends the reply message to make wrong routing direction. It is the Black Hole Attack. Mode 4: Make (N1, M), Broadcast (N1, M). Node N1 generates and broadcasts a large number of messages in a short period of time, leading to normal nodes not working properly. It is DoS Attack. If one behaviour matches the previous defined attack patterns, it is likely to be attack node the role of the decision-making module is to identify attacks, position the invaders, and send out an instruction to its neighbor nodes to arouse the Counterattack Agents. In addition to this the black hole detecting component is used to collect the network node ID of these nodes and to analyze them. Thus it would reduce the time required for black hole detection about a particular node and improve the system performance. In Alert, Responses and cooperative agent module is used to identify the alert level of the node.
1 Serious : Drop the node Id and alert all the neighboring nodes
2 Moderate : Dynamic decision is taken whether to drop the node or not
3 Slight: do not care condition.
4 Layer 4 Application security layer The application security layer refers to the security of End-system, such as security protocols of Secure Socket Layer (SSL),The cooperative and communication agent is used to receive alert messages from other security agents. After receiving these alerts the agent makes a judgment is larger than 0.5 and then adds a new rule to its table Secure Shell (SSH), Secure Electronic Transaction (SET) and others. The protocols are independent of the underlying network security layer, which encrypt the data before it enter into the network layer to ensure data security. In the layer, the security protocol being used is determined by the application
programs running in the system, such as SSL is the protocol to enhance security Web transmission; the SSH is the protocol to enhance security Telnet/FTP transmission. The application security layer is corresponding to four layers from the transport layer to the application layer of OSI model, which defines secure mechanisms related to application programs in the end systems, such as SET protocol, so it is separated from the underlying layers.

ISSN: 2278 – 7798

III. PROPOSED METHOD:

A Semantic Approach to coding in Content Based MANETs

1.By survey we found that fully cache CB –MANET is most appropriate solution for reliable disseminate large files under intermittent connectivity but, performance wise both fully cache and unrestricted coding are on same level[2].

2.Our proposed solution is "A semantic approach CB-MANET" which will use semantic search based GP and creates meaningful understanding among all the nodes (Source as well as intermediate) this will improve the performance of system drastically.

IV. CONCLUSION

By survey we concluded that fully cache CB –MANET is most appropriate solution for reliable disseminate large files under intermittent connectivity but, performance wise both fully cache and unrestricted coding are on same level. Our proposed solution is "A semantic approach CB-MANET" which will use semantic search based GP and creates meaningful understanding among all the nodes (Source as well as intermediate) this will improve the performance of system drastically.

REFERENCES

5. 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] HAO YANG, HAIYUN LUO, FAN YE, SONGWU LU, AND LIXIA ZHANG, "SECURITY IN MOBILE AD HOC NETWORKS: CHALLENGES AND SOLUTIONS", IEEE 2004, pp 38-47

[4] Kejun Liu, Jing Deng, Pramod K. Varshney, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", IEEE 2007, pp. 536-550

[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.

ISSN: 2278 – 7798

[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.

First Author

Ms.Srashti Badkul, M. Tech Student (4th Sem.) from Gyan Ganga Institute of Technology and Sciences, Jabalpur (M.P.). She has published 1 research paper in international journal..

Second Author

Mrs.Brajlata Chourasiya Asst. Professor in Gyan Ganga Institute of Technology and Sciences, Jabalpur (M.P.). I have published 10 research papers in various national and international journals and conferences. Out of these 10, four are from International Journals.

ISSN: 2278 – 7798