NETWORK CODING COMBINED WITH ONION ROUTING FOR ANONYMOUS AND SECURE COMMUNICATION IN A WIRELESS MESH NETWORK

Abhinav Prakash[1], Dharma P. Agrawa[l], and Yunli Chen[2]

Abhinav Prakash[1], Dharma P.Agrawal[1] and Yunli Chen[2], [1]Uni-versity of Cincinnati, USA and [2]Beijing University of Technology, China

ABSTRACT

This paper presents a novel scheme that provides high level of security and privacy in a Wireless Mesh Network (WMN). We combine an approach of Network Coding with multiple layered encryption of onion routing for a WMN. An added superior feature provides higher level of security and privacy. Sensitive network information is confined to 1-hop neighborhood which is available anyways in a wireless medium with nodes using a bivariate polynomial. The only routing information divulged to a relay node is about next hop. No plain text is ever transmitted and all data can only be decrypted by its source and destination. Prior work finds it difficult to enforce encryption with network coding without divulging in complete routing information,hence losing privacy and anonymity. We compare our scheme with other existing approach for several networks. The preliminary results show this work to provide superior security and anonymity at low overhead cost.

INDEX TERMS

Network Coding, Mesh Networks,Onion Routing, Privacy, Security.

I. INTRODUCTION

A Wireless Mesh Network (WMN) consists of Internet Gateways (IGWs), Mesh Routers (MRs) and Mesh Clients (MCs). MCs are served by MRs which are connected together using wireless links in an ad hoc mode and constitute as the backbone of a WMN.Some MRs act as IGWs to provide access to the Internet and makes the network very costeffective. MRs could be of different types, such as Wi-Fi, WiMax routers etc. and could have different interfaces. This leads to two levels of hierarchy, MRs at higher level with many different wireless interfaces, and MCs constitute the lower level and are served by MRs using separate interfaces with the presence of few IGWs wired to the Internet, the cost is low, while easy to expand using additional MRs. In this way, it is easy to expand WMNs, especially in the sparsely populated areas and makes them easily scalable. Another very important application of a WMN is to provide different medium of wireless access. Hence, WMN can be said to be dynamically self-organized and auto-healing.

Versatilities of a WMN is especially important in an open wireless medium where MRs are owned by different independent entities.Such networks mainly rely on an ad-hoc packet transmission mechanism as MRs forward along the route from source to destination acting as relay nodes. Several possible misbehaviorscould be identified as impersonations, packet sniffing, selfish behavior etc. There are several works to date focusing on identifying and

DOI : 10.5121/ijcnc.2014.6601

rectifying many such misbehavior [1]. In this paper we introduce a scheme to utilize the concept of network coding that maximizes efficiency of the WMN with low overheads and high level of security and anonymity by using encryption at each link along the path.

A. Background and Related Work

1) Security: The field of Wireless Mesh Network is still in its early stage and hence security is open. The protocol for WMNs are still to be developed. In a WMN the MRs are pretty static while MCs move around at different speed and get connected to MRs in their vicinity. In the year 2006 [2] described various attacks like sinkhole and wormhole attacks and also look into numerous vulnerabilities of a WMN. Many ideas have been proposed to combat these attacks using different techniques, including shared private keys and public-private key pairs. RSA-based public key cryptography is one example. The Asymmetric key system are complex for authentication and data communication as it is computationally very expensive. Hence, to maintain low energy consumption in MCs with limited energy sources, we want our scheme to be light weighted.

Use of symmetric keys seems to be an attractive option. In [3], Eschenauer and Gligor proposed a random key distribution scheme such that each device randomly selects a group of keys from a large pool of P keys.A major disadvantage of this scheme is that if the number of keys given is small, most of the devices are sparsely connected and are not capable of communicating with each other as they may not have even one key in common. Hence, lots of devices remain disconnected. When the number of keys given is large, the scheme becomes susceptible to a device capture attack. This could force a large amount of secret to be lost, thereby compromising a large portion of the network. Furthermore, each pair of devices to have a shared symmetric key each device must be given at least n-1 common keys to spawn capability of complete connectivity. Chan et al. [4], revised the Eschenauers and Gligors model by having at least q (where q>1) keys in common between two adjacent wireless devices instead of just one common key, so that they can have a secure wireless link between them. They call their scheme to be q-composite random key pre distribution scheme. This is one way to enhance the network resilience against any device capture attack. Blom also introduced a symmetric key generation scheme (SKGS) [5], where a pair of devices can independently generate a common key between them by exchanging a small amount of secret information. However there could be dependencies between the keys in this particular approach and a number of users have to collaborate in resolving the ambiguity of unknown keys. This makes this scheme vulnerable to device capture attack when the number of captured devices exceed a given threshold value which is directly proportional to the amount of secret divulged. In [6], Blundo et al. proposed a secure key distribution scheme for systems where a device may leave or enter the network dynamically, by that constantly changing the network topology. Therefore, they proposed a t-degree bivariate symmetric polynomial pre distribution scheme. Such a strategy is equally pertinent to any hierarchical networks. Usually, the communicating wireless devices swap polynomials by substituting the variables with their respective IDs. It is possible to compute a common secret key between them due to the symmetric attribute of the polynomial. This scheme is called as k-secure where k pertains to the degree of the symmetric polynomial.

Yi Cheng et al. [7] have presented a pair wise key establishment mechanism (EPKEM) by generating keys and arranging them in a matrix so that a common shared key between any communicating nodes can be achieved. Each user is allocated a row and a column of keys to form (2m - 1) set of keys. The selected (2m-1) elements from the matrix are then loaded into each device along with the(i; j) coordinates of the respective elements to form its key ring and then they are deployed randomly. In this scheme, two devices discover a common key between them by broadcasting their respective IDs while the indices (i; j) of keys are exchanged that were used at the time of key pre-distribution. This scheme drastically reduces the number of keys that are needed to be pre-stored on the devices during the deployment phase, while assuring at least two common keys among a pair of any adjacent devices.

2) Preliminaries: Polynomial Based Scheme: In [8], we proposed a bivariate polynomial function based security scheme that is highly scalable at a very low cost. In this scheme, we introduced a novel scheme to allow a secured authenticated connection between any two entities in a WMN. The two adjacent nodes can be an IGW, one MR or any MC. The crucial step of this scheme is to furnish each node a set of bivariate polynomials during the pre-deployment phase by the central authority. Once deployed, this secret polynomial are used to independently generate symmetric secure key and once achieved, we say that the two nodes have an generated an authenticated association with each other. It should be noted that during the pre-deployment phase, three different sets are given to each node as follows:

1) A shared key K for initial secure information exchange.

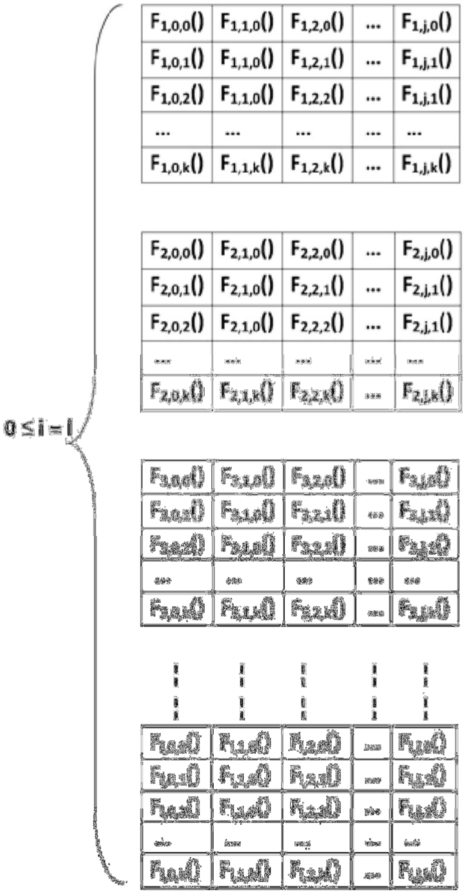
2) A set of Bivariate Polynomial Functions Fi,j,k(x,y)(where 0 i < l; 0 j < m; 0 k < m) picked randomly from a 3D matrix of polynomials and the indices of the selected polynomial functions.
3) A function H( ) known as the hash function to compute the shared key from the values received by the bivariate polynomial functions. This three dimensional matrix has been adapted from Yi Cheng‘s scheme in [7] and [9] by randomly selecting the polynomials. From the get go each device undergoes three stages of
1) Acquiring Secrets.
2) Authenticated Association.
3) Pair-wise secure channel establishment from a Mesh Client to an IGW or the AAA server.
A standard Bivariate Polynomial distribution is construed as follows:

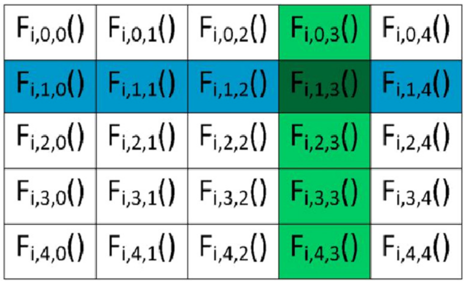
$$F_{i,j,k}(x,y) = \Sigma_{rs=0}^{p} a_{rs} x^r y^s$$

Where the coefficients ars are randomly selected over a Finite Field Gf(X) where X is a very large prime number and i; j; k are the indices for the position of the polynomial in the three-dimensional matrix used at pre-deployment and p is the degree of the function Fi;j;k (x,y). A Polynomial Function is called a Bivariate Polynomial if it satisfies the following elementary prerequisite:

$$F_{i,j,k}(x,y) = F_{i,j,k}(y,x)$$

A three dimensional matrix is conceived containing a bivariate polynomial at each unit position of this matrix. The bivariate polynomi-als selected to populate this three dimensional matrix are randomly chosen from a large pool of such possible bivariate polynomials. For ex-plicit understanding we can contemplate such a matrix as a set of i two dimensional mxm ma-trices with degree t. This allows us to compute





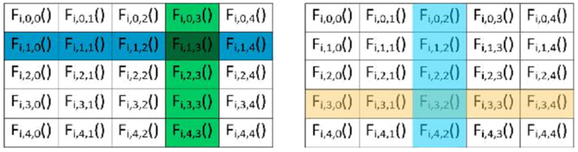
$F_{i,0,0}()$	$F_{i,0,1}()$	$F_{i,0,2}()$	$F_{i,0,3}()$	$F_{i,0,4}()$
$F_{i,1,0}()$	$F_{i,1,1}()$	$F_{i,1,2}()$	$F_{i,1,3}()$	$F_{i,1,4}()$
$F_{i,2,0}()$	$F_{i,2,1}()$	$F_{i,2,2}()$	$F_{i,2,3}()$	$F_{i,2,4}()$
$F_{i,3,0}()$	$F_{i,3,1}()$	$F_{i,3,2}()$	$F_{i,3,3}()$	$F_{i,3,4}()$
$F_{i,4,0}()$	$F_{i,4,1}()$	$F_{i,4,2}()$	$F_{i,4,3}()$	$F_{i,4,4}()$

Fig. 1: A three dimensional matix of bivariate polynomials Fig. 2: A M M Matrix

the total number of bivariate polynomials from a three dimensional matrix as explained below:

Total number of polynomials = l*m*m such that: 0t m and 0 i l We can easily say that a function at the position i; j; k can be written as Fi;j;k(x; y) as displayed in the Figure 1. Now by selecting a set S randomly of matrices containing bivariate polynomials from l, i.e., the total number of m m two dimensional matrices can be obtained as: S d(l + 1)=2e . where dxe is the ceiling function that gives the smallest integer x.Using the ceiling function, We ensure that S is an integer always greater than or equal to l=2. This further guarantees that two different randomly selected sets Sa and Sb always have atleast one m m Matrix in common. After selecting the random set S of matrices with one random column and one random row from each of these matrices in S, all the functions contained in the selected row and column are given to a mesh entity. For example refer Figure2.

Now, since this matrix is of the order m mit has m rows and m columns. So, the number of polynomials contained in one row and one column selected randomly are m + (m 1). Now, there are S such matrices hence total number of bivariate polynomials given to each MC are: The total number of bi-variate polynomials = S (m + (m 1)) = S (2m 1) Now, Let us analyze how two clients on the mesh can have common functions to establish a secure communication channel. Since we know two different set of matrices Sa and Sb have atleast one matrix in common. Let the two common matrices be as shown in Figure 3 Assuming the highlighted rows and columns were randomly selected row and column for sets Sa and Sb respectively. It is obvious that both these sets will have atleast two functions in common. In a better case, there could be more common matrices, leading to more common functions between two mesh entities. So, this technique of allocating polynomials guarantees any two MCs to have atleast two common bivariate polynomial functions which are used for secured communication.



$F_{i,0,0}()$	$F_{i,0,1}()$	$F_{i,0,2}()$	$F_{i,0,3}()$	$F_{i,0,4}()$
$F_{i,1,0}()$	$F_{i,1,1}()$	$F_{i,1,2}()$	$F_{i,1,3}()$	$F_{i,1,4}()$
$F_{i,2,0}()$	$F_{i,2,1}()$	$F_{i,2,2}()$	$F_{i,2,3}()$	$F_{i,2,4}()$
$F_{i,3,0}()$	$F_{i,3,1}()$	$F_{i,3,2}()$	$F_{i,3,3}()$	$F_{i,3,4}()$
$F_{i,4,0}()$	$F_{i,4,1}()$	$F_{i,4,2}()$	$F_{i,4,3}()$	$F_{i,4,4}()$

(a) Sa

$F_{i,0,0}()$	$F_{i,0,1}()$	$F_{i,0,2}()$	$F_{i,0,3}()$	$F_{i,0,4}()$
$F_{i,1,0}()$	$F_{i,1,1}()$	$F_{i,1,2}()$	$F_{i,1,3}()$	$F_{i,1,4}()$
$F_{i,2,0}()$	$F_{i,2,1}()$	$F_{i,2,2}()$	$F_{i,2,3}()$	$F_{i,2,4}()$
$F_{i,3,0}()$	$F_{i,3,1}()$	$F_{i,3,2}()$	$F_{i,3,3}()$	$F_{i,3,4}()$
$F_{i,4,0}()$	$F_{i,4,1}()$	$F_{i,4,2}()$	$F_{i,4,3}()$	$F_{i,4,4}()$

(b) Sb

Fig. 3: Common Matrix between sets Sa and Sb

Achieving a Secure Link for Communi-cation: When the network is formed, each MC identifies its neighbors and exchanges informa-tion to generate a secure key for communica-tion. Say for example, Once two neighbors C and D find each other, they share each others node ID and the indices of the polynomial functions they possess. This information is encrypted using a common Key K which is given to each node for an initial handshake and exchange information to generate a secured key on the fly. Using the polynomial function indices, both the nodes separately determine which function they have in common.

Assuming the node IDs are IDC and IDD and the common functions are F2;7;6() and F2;3;4().
At node C, seed values will be computed using the common functions and node IDs of C and D.

Seed 1C = F2;7;6(IDC , IDD)
Seed 2C = F2;3;4(IDC , IDD)

Similarly, at node D, it would compute its seed values:
Seed 1D = F2;7;6(IDD , IDC)
Seed 2D = F2;3;4(IDD , IDC)

Since functions F2;7;6() and F2;3;4() are bivari-ate polynomial we get using this property:

F2;7;6(x; y) = F2;7;6(y; x)

The same is true for any other common func-tion therefore:

Seed 1C = Seed 1D
Seed 2C = Seed 2D

This is applicable to any further seeds.

So, the seeds generated independently at both the nodes would be identical. Each node uses a one way hashing function Hf() that is assigned during the deployment phase. All the seed values are hashed to generate a final secured key for communication and since the same hash function is used at both the nodes and seed values being identical, they both have the same identical unique

key for encryption or decryption. This key is never sent over the network and is just used for encryption at the sender end and decryption at the receiver which ensures the key not to be stolen by other entities that might be overhearing the communication.
SecureKey = Hf(Seed 1C ; Seed 2C ; : : :)

If the two nodes have more than two common functions, they generate more than two seed values. This provides more than two seed val-ues to the hashing function which makes it even stronger and more secure. In this fashion, all the nodes establish secure encryption technique with their one hop neighbors. Assuming a node A needs to communicate to the Internet Gateway which is five hops away from it. Each of the four links on the way would be a secured connection using pairwise key. This pairwise secure key establishment ensures end-to-end secured transfer.

3) Privacy: A lot of work has been done in the field of security [7], [9] for a WMN. But, multiple vulnerabilities still remain open in the field of privacy. Several researchers have attempted to address the privacy issues related to a wired network and there seems to have a lot of scope in this field especially in a wireless network scenario. For example, in a wired network, Onion Routing [10] was invented by Michael G. Reed, Paul F. Syverson, and David M. Goldschlag to provide anonymity of destination. In this scheme, a path is pre-computed at the source and the data packet is encrypted in multiple layers with the public key of the forwarding node along the path to destination in a sequential order and each node removes their layer of encryption after receiving the packet and forward the remaining packet called the onion to the next hop and finally the decrypted data with all the layers of encryption removed, received by the des-tination. The work in [11] resorts to a quan-titative approach towards privacy. Authors in [12] specifically approach provisions for pri-vacy preservation but lack efficiency of gains achieved from the network coding. The basis of privacy performance parameters are well defined in [13].

In [14], Wu and Li introduced an onion ring protocol for wireless mesh networks where onion rings are formed starting at the IGW and using all the cycles in the network. Data only travels in one direction and data sessions are only initiated at the gateway router. This provides a good anonymity, while fails on several issues such as a bottleneck is created at the gateway router as all the scheduling is done at the gateway. Moreover, this scheme works on the concept of finding cycles. In a dynamic WMN, uplink messages are initiated at the MR to traverse through the network to the IGW, which could fail in a realistic scenario. Another problem in this protocol is all the other nodes in a ring have to wait while one node communicates.

The work [15] talks about a layered onion ring approach in which some routers are con-sidered trusted nodes and is similar to [14]. Communication starts and ends at the MR and

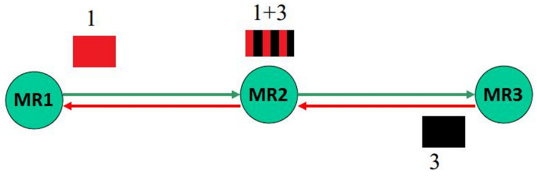


Fig. 4: Coding Gain with oppurtunistic listen-ing Example 1

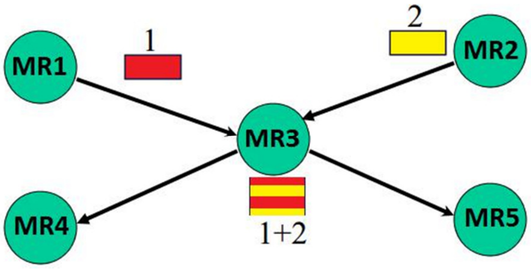


Fig. 5: Coding Gain with oppurtunistic listen-ing Example 2

some level of anonymity is present in the net-work. But, this work strongly relies on finding the cycles in the network.

4) Random Linear Network Coding: In Random Linear Network Coding (RLNC), par-ticipating nodes combine their incoming pack-ets linearly using randomly chosen coefficients. It has been observed to be very efficient with reference to the network coding exemplar [16]. The basic idea behind network coding is when a node overhears multiple incoming packets, it simultaneously places a linear combination of all the overheard packets and retransmits this single coded packet which when received, can be decoded to obtain original packets if sufficient information is available at the decod-ing node. Example of coding gain achieved as explained in [17] is shown in Figures 4 and 5. Intuitively, these gains are huge and open new doors to multicast networks like P2P and WMN's. As any new superior technology not only does it create several new possibilities and strengths to wireless networks, it also opens new doors for exploiting new security and privacy schemes. Inherently network coding approach does provide some security due to its intrinsic nature. But, being an application for content distribution efficiently it works on co-operative networking and all nodes are trusted with sharing several parameters for information extraction which faced with any smart mali-cious node fails miserably. Intrinsically Net-work Coding approach has a huge conflict with strong anonymous schemes like onion routing and are actually unusable in their original form. Our approach modifies both these well known schemes and combines them together to work cooperatively while removing any conflicts sys-tematically. Some existing similar approaches employing network coding and achieving pri-vacy can be found in [18] and [19]. Authors in [20] introduce an enhanced scheme for network coding and promise even superior gains. The work in [21] achieves groundbreaking results in deploying network coding for a realistic wireless network and provides huge gains over conventional packet forwarding mechanisms. In our proposed scheme, we use the foundation of network coding using XOR scheme. This work is our further enhancement to the work previously published in [22].

II. PROPOSED SCHEME: NETWORK CODING ON MODIFIED ONION ROUTING

We assume that all MCs have Omni-directional Antenna with uniform transmis-sion range. Network Initiation takes place with neighborhood discovery by MCs, MRs and IGW's. Each MC discovers its one hop neigh-bor MR's which we define as a neighborhood as given in Table I. Our scheme has two

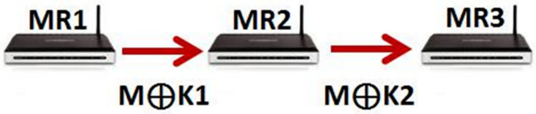


Fig. 6: Message Propagation

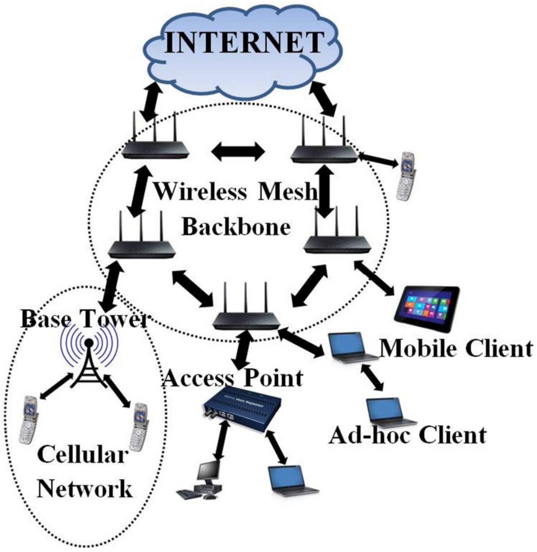


Fig. 7: A Wireless Mesh Network

salient features. First, a group key is generated using bivariate polynomial among devices in a neighborhood. The second step is to merge the message with the group key similar to network coding so that actual message is never transmitted, but extracted at each intermedi-ate MR as illustrated in Figure 6. When the message propagates from MR1 to MR2 and so on. As MR2 knows the group key K1 between two MRs, the message can be easily extracted. Then, MR2 encrypts message by mixing with K2 similar to network coding and so on till the message reaches the IGW.

A. Network Initiation

Network initiation starts with one hop neigh-bor discovery and creating authenticated secure communication paths. Each MC registers its membership with the MR over a secure communication channel. After MC's registration is complete MR processes the network map creating a uniform spanning tree with branches of the tree that gives routes going through various MRs and eventually to an IGW.

Having multiple MRs makes our scheme

TABLE I: A Branch Table Entry

BID	Nextid	Previd
34	A3E	C5F

even stronger as it enables routers to work cooperatively while providing higher privacy and sharing the load. In such cases branches starting and ending in a MR can be created for the network topology of Figure 7 and the corre-sponding network model of Figure 9. Creating such Neighborhoods gives the scheme multiple strengths. All the members of the neighborhood that are a part of a path in which data flows, is illustrated in Figure 8.

III. IMPLEMENTATION DETAILS

This section describes how our scheme reacts in different network scenarios and how network coding is intertwined with onion routing using onion packets providing very high level of privacy at a low cost and achieving the cod-ing gain utilizing opportunistic listening and coding as in [17]. In our proposed scheme we have segregated MRs into one-hop neighbor-hoods. This logical network sectioning makes our scheme robust and distributed hence ideal for a Wireless Mesh Scenario.

We use a similar network coding scheme as proposed in COPE in [17]. Additionally we empower the relay nodes by providing just enough information to be capable of decipher-ing routing information to the next hop in the correct direction towards the destination node. This is achieved without disclosing a source-destination pair and the payload of the data packet. At the same time a relay node is capable of opportunistically decoding and encoding data packet again together but with a very different key. This makes the COPE [17] coding scheme even more efficient and utilizes lower overheads while keeping high gains.

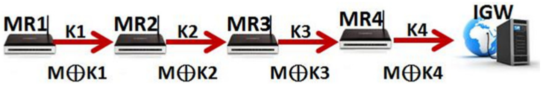


Fig. 8: Route for Mesh Routers to IGW

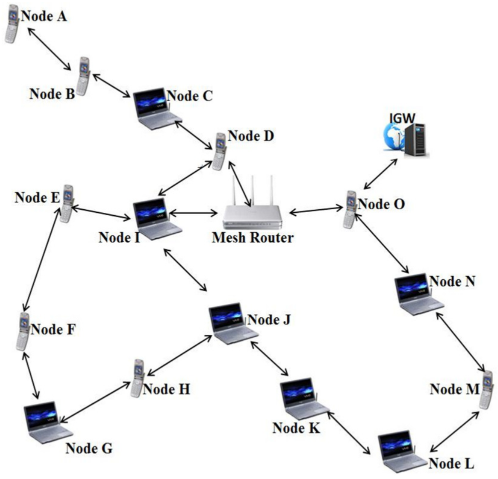


Fig. 9: Network Map at MR (center)

IV. PERFORMANCE ANALYSIS

In [8], we have shown that our PBS (polynomial based scheme) is highly scalable and perfectly secure which is provided at a very low cost. With very few functions stored on a MC, we can support a very large network. The proposed Network Coding combined with Onion Routing(NC&OR) scheme takes this to the next level and fills the gap of privacy in case of an attack by a global adversary. Very high level of anonymity is achieved at the cost of an incremental overhead, like decryption and encryption with a new key at each stage. The overheads are caused by Multiple Encryption as per onion routing. It can be easily observed that the onions incur a heavy cost of usage. But, in NC&OR, we only use forward path. This helps us in keeping the cost to bare minimum for multiple encryptions as compared to a pure onion ring routing in [14] and layered onion ring routing approach of [15] where they always use onions for any type of communication. Redundancy in Network Coding and Modified Onion Routing is much more efficient than Phantom Routing of [23] which is based on flooding to ensure privacy among a group of nodes that necessitates too many re-transmissions.

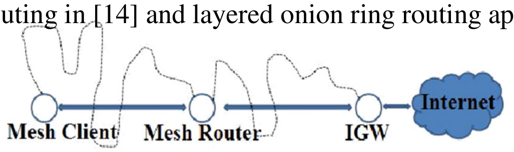


Fig. 10: A Packet Propagation Path from Clientto IGW

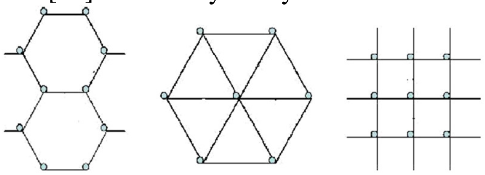


Fig. 11: Regular MC Deployment in Hexagon, Triangle and Square Patterns

Anonymity:

To an outside observer, all the MRs in a WMN act exactly the same way. The encrypted communication combined with the usage of dummy packets makes it impossible even for the global observer [24] to isolate the node initiating the communication session. Additionally, a session is never initiated at the MC as it can only request for a session to a MR. In case of presence of an inside attacker, information can not be leaked as each MC only knows about the 1-hop information among the branch (previous and next entity). The data packets are forwarded by an inside attacker and are encrypted. Hence, a dummy packet and a data packet are indistinguishable by an inside attacker as they appear exactly the same in their encrypted form.

In our scheme, the flow of traffic goes through two layers of branches which makes it impossible to isolate the session initiator. It randomly propagates the packet towards the IGW. In our case, the selection of branches on different levels is totally independent which makes it difficult to predict what path the packet is going to take by each MR. Addi-tionally, availability of multiple branches adds further randomization to the selection of the final path taken. Multiple layers and availability of several branches makes our scheme more or less private and secure. Furthermore, each encryption key can be changed dynamically over time, using the bivariate polynomial.

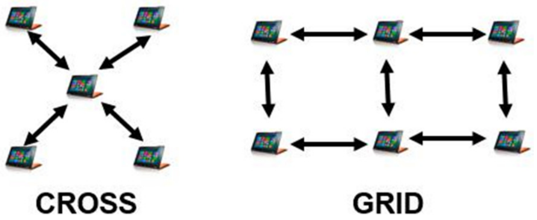


Fig. 12: Regular Network Topology

Experimental Results:

We now evaluate our scheme using realistic wireless settings. Our evaluation is based on applying real network metrics into the well known ns-2 network simulator. In our exper-iment two types of nodes are deployed. A MR acting as the sync node and rest of the MRs are all relay nodes with network coding capabilities and few nodes are randomly selected to act under an active session with the MR. We compare our scheme with the following two routing protocols:

1. COPE, the routing protocol with network coding (simulated by using our algorithm without any encryptions under same constraints and parameters),

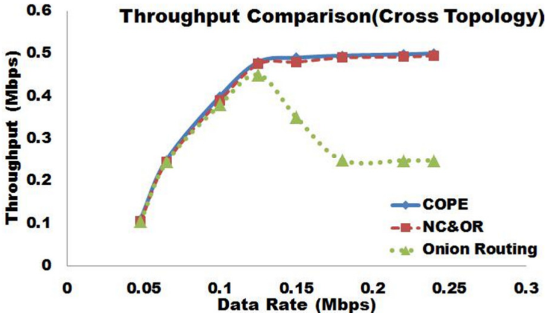


Fig. 13: Average Throughput in Cross Topol-ogy

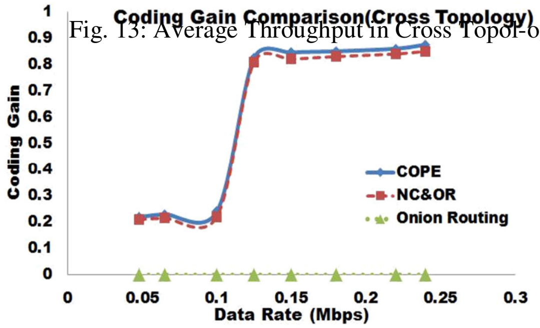


Fig. 14: Coding Gain Achievement Compari-son in Cross Topology

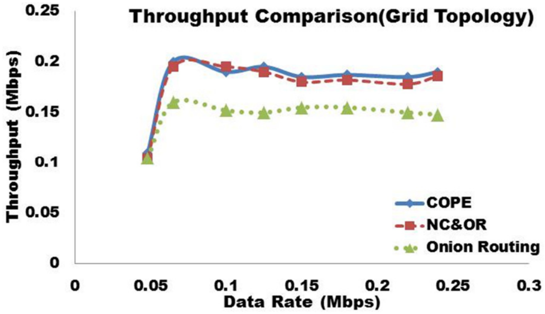


Fig. 15: Average Throughput in Grid Topology

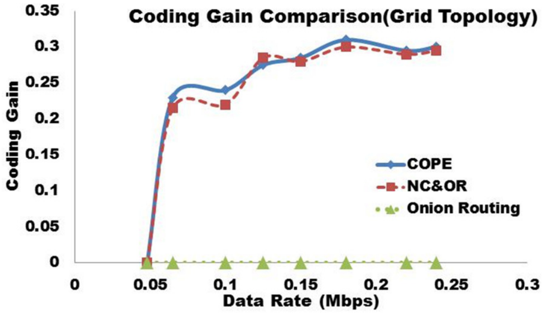


Fig. 16: Coding Gain Achievement Compari-son in Grid Topology

2. TOR (The Onion Routing) protocol be-tween initiating MR and IGW with no network coding (simulated by using our algorithm with-out any network coding under same constraints and parameters).

Our results are compared on the basis of performance in these three parameters:

1.Average Throughput over entire runtime.
2.Coding Gain (Fraction of total packets that were coded before forwarding)
3.Encryption/Decryption Cost, the computa-tional cost of packet processing when encryp-tion is used.

With our earlier experience with regu-lar network deployments [25], we considered three standard deployments namely: Triangular, Square and Hexagonal as displayed in Figure 11. Triangular and Hexagonal deployments es-sentially break down into the cross topology and square deployment is represented by the grid topology as shown in Figure 12. We used all default seed values of 802.11b wireless networking specification using UDP data pack-ets with transmission range is set to 250m. Results are averaged over 15 simulations for each setup. Graphs 13, 14, 15, and 16 show how our scheme Network Routing and Onion Routing (NC&OR) gives high level of coding gain almost equivalent to COPE while main-taining Onion Routing's high level or security and privacy. Further we deduce from our results that Cross topology outperforms Grid topology.

V. CONCLUSION

In this paper, we propose solution to an sub-stantial problem that when a wireless network unfolds network coding, previously operational privacy-sustaining methods no longer operate correctly or are left non-functioning. To this end, we propose a superior hybrid scheme which combines the strengths of onion rout-ing and embedding it with Network Coding , a contemporary anonymous communication protocol which can function for distributed dynamic wireless networks. Both analytical and experimental results suggest that our scheme not only keeps the advantage of network coding for an effective use of the capacity, but also ensures enhanced privacy for MCs without much overhead.

VI. FUTURE WORK

Our proposed scheme encounters various complex network scenarios in a random net-work topology scenario. The research work is ongoing in a realistic random deployed WMN.

Preliminary results obtained experi-mentally show promising prospects for high gains and efficient performance of our scheme NC&OR in a random WMN.

ACKNOWLEDGMENT

The authors would like to thank members of the Center of Distributed and Mobile Comput-ing Lab (CDMC) at the University of Cincin-nati for their technical feedback which helped improve the presentation.

REFERENCES

[1] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. Agrawal, “Wireless mesh networks: Current challenges and future directions of web-in-the-sky,” Wireless Communications, IEEE, vol. 14, pp. 79 –89, august 2007.

[2] Y. Zhou and Y. Fang, “Security of ieee 802.16 in mesh mode,” in Military Communications Conference, 2006. MILCOM 2006. IEEE, pp. 1 –6, oct. 2006.

[3] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proceedings of the 9th ACM conference on Computer and communica-tions security, CCS ’02, (New York, NY, USA), pp. 41– 47, ACM, 2002.

[4] H. Chan, A. Perrig, and D. Song, “Random key predis-tribution schemes for sensor networks,” in Security and Privacy, 2003. Proceedings. 2003 Symposium on, pp. 197 – 213, may 2003.

[5] R. Blom, “An optimal class of symmetric key generation systems,” in Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of crypto-graphic techniques, (New York, NY, USA), pp. 335–338, Springer-Verlag New York, Inc., 1985.

[6] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vac-caro, and M. Yung, “Perfectly-secure key distribution for dynamic conferences,” in CRYPTO, pp. 471–486, 1992.

[7] Y. Cheng and D. Agrawal, “Efficient pairwise key estab-lishment and management in static wireless sensor net-works,” in Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, pp. 7 pp. –550, nov. 2005.

[8] A. Gaur, A. Prakash, S. Joshi, and D. P. Agrawal, “Polynomial based scheme (pbs) for establishing au-thentic associations in wireless mesh networks,” Journal of Parallel and Distributed Computing, vol. 70, no. 4,
pp.338 – 343, 2010.

[9] Y. Cheng, M. Malik, B. Xie, and D. P. Agrawal, “En-hanced approach for random key pre-distribution in wire-less sensor networks,” in Proceedings of International Conference on Communication, Networking and Infor-mation Technology, 2008.

[10] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, “Onion routing network for securely moving data through communication networks,” 07 2001.

[11] Y. Li, J. Ren, and J. Wu, “Quantitative measurement and design of source-location privacy schemes for wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 7, pp. 1302–1311, 2012.

[12] Z. Wan, K. Ren, B. Zhu, B. Preneel, and M. Gu, “Anonymous user communication for privacy protection in wireless metropolitan mesh networks,” Vehicular Tech-nology, IEEE Transactions on, vol. 59, pp. 519–532, Feb 2010.

[13] K. Vu, R. Zheng, and J. Gao, “Efficient algorithms for k-anonymous location privacy in participatory sensing,” in INFOCOM, 2012 Proceedings IEEE, pp. 2399–2407, March 2012.

[14] X. Wu and N. Li, “Achieving privacy in mesh networks,” in Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, SASN ’06, (New York, NY, USA), pp. 13–22, ACM, 2006.

[15] R. Li, L. Pang, Q. Pei, and G. Xiao, “Anonymous com-munication in wireless mesh network,” in Computational Intelligence and Security, 2009. CIS ’09. International Conference on, vol. 2, pp. 416 –420, dec. 2009.

[16] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” Information Theory, IEEE Trans-actions on, vol. 52, pp. 4413–4430, Oct 2006.

[17] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, “Xors in the air: Practical wireless network coding,” Networking, IEEE/ACM Transactions on, vol. 16, pp. 497–510, June 2008.

[18] P. Zhang, C. Lin, Y. Jiang, P. P. C. Lee, and J. C. S. Lui, “Anoc: Anonymous network-coding-based commu-nication with efficient cooperation,” IEEE Journal on Selected Areas in Communications, pp. 1738–1745, 2012.

[19] J. Wang, J. Wang, C. Wu, K. Lu, and N. Gu, “Anony-mous communication with network coding against traffic analysis attack,” in INFOCOM, 2011 Proceedings IEEE, pp.1008–1016, IEEE, 2011. 11

[20] T. Cui, L. Chen, and T. Ho, “Energy efficient opportunis-tic network coding for wireless networks,” in INFOCOM 2008. The 27th Conference on Computer Communica-tions. IEEE, April 2008.

[21] J. C. Corena, A. Basu, S. Kiyomoto, Y. Miyake, and T. Ohtsuki, “Xor network coding pollution prevention without homomorphic functions,” in Consumer Com-munications and Networking Conference (CCNC), 2014 IEEE 11th, pp. 293–300, Jan 2014.

[22] A. Prakash, A. Gaur, and D. P. Agrawal, “Multilevel onion tree routing for anonymous and secure commu-nication in a wireless mesh,” Cyber Journals: Multidis-ciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), vol. 3, January 2013.

[23] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhanc-ing source-location privacy in sensor network routing,” in Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, pp. 599 –608, june 2005.

[24] K. Mehta, D. Liu, and M. Wright, “Protecting location privacy in sensor networks against a global eavesdrop-per,” Mobile Computing, IEEE Transactions on, vol. 11, pp. 320 –336, feb. 2012.

[25] Y. Wang and D. P. Agrawal, “Optimizing sensor networks for autonomous unmanned ground vehicles,” Optics/Pho-tonics in Security and Defense, (Cardiff, Wales, United Kingdom), vol. 7112, pp. 15 –18, Sep. 2008.

AUTHORS

Abhinav Prakash is a PhD student in the Computer Science Division at the University of Cincinnati. He is working for his doctorate under the guidance of Dr. Dharma P. Agrawal at the Center for Development of Mobile Comput-ing(CDMC) Lab a part of EECS depart-ment at University of Cincinnati. He has a Bachelors in Computer Science from Banaras Hindu University in India and a Masters of Science in Computer Science from University of Cincinnati. His research interests include distributed systems, security in sensor and mesh networks, and applications of parallel computing.

Dharma P. Agrawal is the Ohio Board of Regents Distinguished Professor and the founding director for the Center for Distributed and Mobile Computing in the EECS department, University of Cincinnati, OH. He is a coauthor of textbooks on Introduction to Wireless and Mobile Systems, 4th edition and Ad hoc and Sensor Networks, 2nd edition.His recent research interests include resource allocation and security in mesh networks, efficient deployment and security in sensor networks, use of Femto cells, and heterogeneous wireless networks. He has seven approved patents, two personal pending patents and twenty four patent filings in the area of wireless cellular networks. He has been the Program Chair and General Chair for numerous international conferences and meetings. He is a Fellow IEEE 1987; ACM 1998; AAAS 2003; WIF 2004, and Charter Fellow, National Academy of Inventors, 2012 and is recipient of the IEEE-CS 2008 Harry H. Goode Memorial Award.

Yunli Chen received her BS, MS and Ph.D. degrees from Zhejiang University, China, Beijing Institute of Technology, China and University of Cincinnati in 1994, 1999 and 2004 respectively. From 2004 to 2008, she was with Motorola. Currently, she is an associate professor with Beijing University of Technology, where she conducts research and development of MAC, routing, and transport protocols for wireless mesh networks. Her research interests also include cross-layer design, energy efficient power allocation and communication protocols for cellular, mobile ad hoc, and sensor networks