An Analysis on Multihop Wireless Networks

D.sanjeevkumar[1],T.Sathiyaseelan[2], Saravana Kumar P S[3] ,Saravana Kumar R[4]

SNS College of Technology, Coimbatore, Tamilnadu, India

Sanjeevkumarsanj9774@gmail.com

Abstract: **The multi-hop wireless networks at all times having security problems; the network traffic causes the attacks in inside attackers and outside attackers, to avoid those attacks by using navel network coding techniques. Coding and mixing operation was encouraged in intermediate nodes. Data splitting and transmitting is done in network coding algorithm. The proposed scheme provides the packet flow intractability and message content confidentiality is ensured by threshold secret sharing algorithm. Traffic analysis presents a serious threat in Multi-hop wireless networks privacy, where attacks such as traffic analysis and flow tracing can be easily launched by a malicious adversary due to the open nature wireless medium. Traditional solutions are mainly based on the mix mechanism, but the main drawback is its low network performance due to mixing and cryptographic operations. In this paper, we propose a novel network coding based privacy-preserving scheme against traffic analysis in Multi-hop wireless networks. With homomorphic encryption on Global Encoding Vectors (GEVs), the proposed scheme offers two significant privacy-preserving features, packet flow untraceability and message content confidentiality, for efficiently thwarting the traffic analysis attacks. Moreover, the proposed scheme keeps the random coding feature, and each sink can recover the source packets by inverting the GEVs with a very high probability. Theoretical analysis and simulative evaluation demonstrate the validity and efficiency of the proposed scheme.**

Keywords: **Network coding, Traffic analysis, Threshold secret sharing.**

I. INTRODUCTION

Wireless Access Networks(WAN), such as Wi-Fi, have been widely deployed due to their convenience, portability, and low cost. However, they still suffer inherent shortcomings such as limited radio coverage, poor system reliability, and lack of security and privacy. In addition, some advanced attacks, such as traffic analysis and flow tracing, can also be launched by a malicious adversary to compromise users' privacy, including source anonymity and traffic secrecy. In this paper, we focus on the privacy issue, i.e., how to prevent traffic analysis/flow tracing and achieve source anonymity in MWNs. Among all privacy properties, source anonymity is of special interest in MWNs. Source anonymity refers to communicating through a network without revealing the identity or location of source nodes. Preventing traffic analysis/flow tracing and provisioning source anonymity are critical for privacy aware MWNs, such as wireless sensor or tactical networks. Consider a simple example of multicast communication in military ad hoc networks, where nodes can communicate with each other through multi-hop packet forwarding. If an attacker can intercept packets and trace back to the source through traffic analysis, it may disclose some sensitive information such as the location of critical nodes (e.g., the commanders) and then further it may impair the location privacy. Subsequently, the attacker can take a series of actions to launch the so called Decapitation Strike to destroy these critical nodes.

A. PARAMETRIC PROBABILISTIC SENSOR NETWORK ROUTING

The need for communication between a regular sensor, called source, and the powerful sensor, called destination can arise at any time possibly triggered by unexpected changes in the environment variable or by a timer; we assume that a communication session consists of sending a single packet of data to the powerful sensor who then forwards it to the base station; this assumption is reasonable as the data of an environmental variable only consist of a few bytes. If a source sends out its data packet, chances are that the packet will not reach the destination in a single hop due to the typically very limited transmission range of the source; in order to obtain a functioning system, other sensors that receive the packet transmitted by the source need to forward the data packet themselves until it reaches the destination. This model of communication results in a multi-hop path from source to destination with intermediate sensors forwarding the packet. Traditionally, if a source and a destination are given, most routing protocols particularly in ad hoc networks first compute a routing path and then route data packets along the computed path. In our setting, this approach seems to be somewhat overkill as we only need to send a single packet to the destination. In fact, a straight-forward flooding approach (i.e., every sensor who receives the packet retransmits it to all its neighbours) would solve our routing problem, but at the cost of involving all sensors in every transmission and thus unnecessarily depleting their batteries.In this paper, we propose a family of routing protocols called Parametric Probabilistic Sensor Network Routing protocols, which substantially improve the performance of controlled flooding methods like gossiping by making the probability of retransmission a function of several parameters. Parametric Probabilistic Sensor Network Routing protocols are completely described by the retransmission probability function: each node in the network upon receiving a packet retransmits the packet to its neighbours with a certain probability according to the probability function. While this basic principle is straight-forward, we must be careful not to overload the probability function: the retransmission probability could depend on parameters as diverse as the numbers of copies of the packet already received by a certain node or the distance to the destination.

B. ANONYMOUS NETWORKING WITH MINIMUMLATENCY

Anonymous networking refers to communication on a network without revealing the source-destination pairs or the paths of traffic flow. While contents of a message can be protected using encryption, hiding the act of communication requires a redesign of underlying network protocols. Changes in communication protocols can affect the quality of service in a network and it is necessary to minimize the loss in network performance while providing anonymity. In particular, protection against information retrieval from arrival and departure times of packets requires modification to the transmission schedules of nodes, which in turn increases network latency.In this paper, we consider the design of node transmission schedules that provide anonymity to network routes with minimum increase in network latency. In particular, we are interested in characterizing the trade-off between the level of anonymity that can be provided and the average latency incurred in a multi-hop network. Anonymous communication systems have typically been designed using Chaum Mixes. A Mix is a node or server that collects packets from multiple users and outputs them in a manner that makes it infeasible to correlate an outgoing packet with a unique incoming packet. Specifically, a Mix performs re-encryption and packet padding to obfuscate the contents of each packet. Further, the Mix also changes the timing pattern of arrived packets by reordering and batching packets from multiple users together. According to the original batching strategy as proposed by Chaum, the Mix waits until at least one packet arrives from n different users before transmitting them all together in a batch. As is evident, the delay incurred by this Mix is potentially unbounded. Although improved batching strategies have been designed, notably by maintaining a pool of packets and flushing a fraction of them periodically, the delay incurred due to the mixing strategies has not been analyzed or optimized.A similar approach was also considered for a wireless multi-hop network in, where bounds were derived on the efficiency of using a fixed transmission schedule. Although fixed scheduling ensures complete anonymity, the high rate of dummy transmissions required makes it energy inefficient and unattractive for large networks. In the context of bandwidth constrained multi-hop networks, the following questions are yet to be addressed, particularly from a theoretical perspective.

II. PROBLEM STATEMENT

Observation of the current work situation will provide clues to problems and atmosphere. Record searching, special purpose records and sampling will give quantitative information about the system which facilitates sizing of the proposed system and may also point the areas of difficulties which are being experienced. Questionnaires can be used to collect the quantifiable data about the system. All of the techniques need to be supplemented by more detailed discussion of the interview situation.Based on the above fact finding techniques, it is observed the current situation of the existing system. It is very helpful to finding the areas of difficulties, which are being experienced in the existing system. Thus it helps to develop the proposed system with the quantifiable data.

A. SYSTEM ANALYSIS

Due to the open wireless medium, MWNs are susceptible to various attacks, such as eavesdropping, data modification/injection, and node compromising. These attacks may breach the security of MWNs, including confidentiality, integrity, and authenticity. Privacy threat is one of the critical issues in multi-hop wireless networks, where attacks such as traffic analysis and flow tracing can be easily launched by a malicious adversary due to the open wireless medium. Network coding has the potential to thwart these attacks since the coding/mixing operation is encouraged at intermediate nodes. However, the simple deployment of network coding cannot achieve the goal once enough packets are collected by the adversaries. On the other hand, the coding/mixing nature precludes the feasibility of employing the existing privacy preserving techniques, such as Onion Routing. Existing privacy-preserving solutions, such as proxy based Schemes Chaum’s mix-based schemes and onion-based schemes may either require a series of trusted forwarding proxies or result in severe performance degradation in practice. We propose a novel network coding based privacy-preserving scheme against traffic analysis in multi-hop wireless networks. With homomorphism encryption on Global Encoding Vectors (GEVs), the proposed scheme offers two significant privacy preserving features, packet flow intractability and message content confidentiality, for efficiently thwarting the traffic analysis attacks. Moreover, the proposed scheme keeps the random coding feature, and each sink can recover the source packets by inverting the GEVs with a very high probability.

B. A SURVEY ON SENSOR NETWORKS

Recent advances in wireless communications and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks. Sensor networks represent a significant improvement over traditional sensors. A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrains or disaster relief operations.On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.The above described features ensure a wide range of applications for sensor networks. Some of the application areas are health, military, and home. In military, for example, the rapid deployment, self-organization, and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military command, control, communications, computing, intelligence, surveillance, reconnaissance, and targeting systems. In health, sensor nodes can also be deployed to monitor patients and assist disabled patients. Some other commercial applications include managing inventory, monitoring product quality, and monitoring disaster areas. Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited to the unique features and application requirements of sensor networks.

C. MULTI-HOP WIRELESS NETWORK

Multihop wireless networks refer to wireless networks where the nodes Collaborate in order to enable the communication between distant (no-connected) nodes. Multihop wireless networks comprise a wide variety of scenarios where they can be used. Depending on the capabilities and characteristics of the nodes that form the network, multihop wireless networks can be classified in wireless mesh networks, wireless sensor networks and Mobile Ad hoc NETworks (MANET).An additional problem of traditional routing schemes relies on the supposition that the network is connected, that is, there is an end-to-end path between any source and any destination. However, node mobility, node sparseness or the propagation variations could lead to situations where the network is disconnected. Under these circumstances, traditional routing protocols are unable to operate. However, the communication could be effective if intermediate nodes store the message to send and they get connected to the final destination in a near future.Opportunistic routing protocols present a promising scheme to improve the wireless network performance by exploiting the broadcast nature of the medium. The main concern of theses protocols relies on which neighboring nodes should forward the data packets and how to coordinate them to avoid duplicated retransmissions. The way to select the relays is supported by metrics. This paper has reviewed the main proposals for multihop ad hoc networks and we have classified them according to the kind of metric used. We can see that the geographic and link-quality based routing protocols have been extended by coding opportunistic routing protocols.

III. PROPOSED WORK

Fact Finding in the methods of gathering the information required about the existing system. Some of them are as follows:

- Observation
- Record Searching
- Special purpose Records
- Sampling
- Questionnaires
- Interviewing

Observation of the current work situation will provide clues to problems and atmosphere. Record searching, special purpose records and sampling will give quantitative information about the system which facilitates sizing of the proposed system and may also point the areas of difficulties which are being experienced. Questionnaires can be used to collect the quantifiable data about the system. All of the techniques need to be supplemented by more detailed discussion of the interview situation.

Based on the above fact finding techniques, it is observed the current situation of the existing system. It is very helpful to finding the areas of difficulties, which are being experienced in the existing system. Thus it helps to develop the proposed system with the quantifiable data.

The first step in developing anything is to state the requirements. This applies just as much to leading edge research as to simple programs and to personal programs, as well as to large team efforts. Being vague about your objective only postpones decisions to a later stage where changes are much more costly.

The problem statement should state what is to be done and not how it is to be done. It should be a statement of needs, not a proposal for a solution. A user manual for the desired system is a good problem statement. The requestor should indicate which features are mandatory and which are optional, to avoid overly constraining design decisions. The requestor should avoid describing system internals, as this restricts implementation flexibility.

Most problem statements are ambiguous, incomplete, or even inconsistent. Some requirements are just plain wrong. Some requirements, although precisely stated, have unpleasant consequences on the system behaviour or impose unreasonable implementation costs. Some requirements seem reasonable at first but do not work out as well as the request or thought. The problem statement is just a starting point for understanding the problem, not an immutable document. The purpose of the subsequent analysis is to fully understand the problem and its implications. There is no reasons to expect that a problem statement prepared without a fully analysis will be correct.

The analyst must work with the requestor to refine the requirements so they represent the requestor's true intent. This involves challenging the requirements and probing for missing information. The psychological, organizational, and political considerations of doing this are beyond the scope of this book, except for the following piece of advice: If you do exactly what the customer asked for, but the result does not meet the customer's real needs, you will probably be blamed anyway.

A. HOMOMORPIC ENCRYPTION

Homomorphic encryption is a form of encryption where a specific algebraic operation performed on the plaintext is equivalent to another (possibly different) algebraic operation performed on the cipher text. For instance, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers. Although a cryptosystem which is unintentionally homomorphic can be subject to attacks on this basis, if treated carefully homomorphism can also be used to perform computations securely. Homomorphic encryption schemes are malleable by design. The homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions, and private information retrieval schemes and enable widespread use of cloud computing by ensuring the confidentiality of processed data.

B. GLOBAL ENCODING VECTOR (GEV)

Each packet transmitted over the network is a linear combination of the original packets R= $\{p_1, p_2, \dots, p_h\}$ generated by the source node s. Accordingly for each edge e ϵ E we define the global encoding vector $\Gamma_e = [\gamma_1^e \dots \gamma_h^e] \;\epsilon\; F_q^h$, that captures the relation between the packets p_e transmitted on edge e and the original packets in R;

$$\mathrm{p_e} = \sum_{i=1}^{h} \mathrm{p_i} \, . \, \upgamma_\mathrm{i}^\mathrm{e}$$

a. Advantages

A communication model in which each intermediate node can only forward incoming packets.

The coding advantage captures the benefit of the network coding techniques for increasing the overall throughput of the network.

For undirected networks, the coding advantage is upper bounded by two. For multiple unicast connections in directed networks it is easy to show that the coding advantage can be as large as the number of unicast pairs.

B. RANDOMIZED MULTIPATH DELIVERY

We consider a three-phase approach for secure information delivery in a WSN: secret sharing of information, randomized propagation of each information share, and normal routing (e.g., min-hop routing) toward the sink. More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares, according to a threshold secret sharing algorithm. Each share is then transmitted to some randomly selected neighbour. That neighbour will continue to relay the share it has received to other randomly selected neighbours, and so on. In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the TTL field is reduced by 1. When the TTL value reaches 0, the last node to receive this share begins to route it toward the sink using min-hop routing. Once the sink collects at least T shares, it can reconstruct the original packet.

C. RANDOM PROPAGATION OF INFORMATION SHARES

To diversify routes, an ideal random propagation algorithm would propagate shares as depressively as possible. Typically, this means propagating the shares farther from their source. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. The challenge here lies in the random and distributed nature of the propagation: a share may be sent one hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from a security standpoint. To tackle this issue, some control needs to be imposed on the random propagation process.

D.ENERGY EFFICIENCY OF THE RANDOM PROBAGATION MODEL

Energy consumption for delivering one bit over one hop is a constant q. Then the average energy consumption for delivering one packet from source s to sink o depends on the average length (in hops) of the route. Note that each random route consists of two components. The first is a fixed Nhop component attributed to the random propagation operation. The second component involves sending the share from the last random relay node.

IV. DESIGNING DESCRIPTIONS

Design is a meaningful engineering representation of something that is to be built. Software design is a process through which the requirements are translated into a representation of the software. Design is the place where quality is fostered in software engineering. Design is the perfect way to accurately translate a customer's requirement in to a finished software product. Design creates a representation or model, provides detail about software data structure, architecture, interfaces and components that are necessary to implement a system. This chapter discusses about the design part of the project. Here in this document the various UML diagrams that are used for the implementation of the project are discussed.

A. ALGORITHMS USED

HOMOMORPHIC ENCRYPTION

We propose a solution by a fully homomorphic encryption scheme. This notion, originally called a privacy homomorphism, was introduced by Rivest, Adleman and Dertouzous shortly after the invention of RSA by Rivest, Shamir, and Adleman. Basic RSA is a multiplicatively homomorphic encryption scheme, i.e., given RSA public key pk=(N,e) and cipher texts $\{\Psi_i \leftarrow \pi_i^e \; mod \; N\}$, one can efficiently compute $\prod_i \Psi_i = (\prod_i \pi_i)^e \; mod \; N$, a cipher that encrypts the product of the original plaintexts. One imagines that it was RSA's multiplicative homomorphism, an accidental but useful property that led Rivest et al, to ask a natural equation: what can one do with an encryption scheme that is fully homomorphic: a scheme ε with an efficient algorithm Evaluate ε that, for any valid public key pk, any circuit C (not just a circuit consisting of multiplication gates as in RSA), and any ciphertexts,

$\Psi_i \leftarrow Encrypt$ ε$(pk, \pi_i$), outputs $\Psi \leftarrow Evaluate$ ε $(pk, C, \Psi_1, \ldots, \Psi_t)$, a valid encryption of C$(\pi_1, \ldots, \pi_t)$.

At a high level, the essence of fully homomorphic encryption is simple: given cipher texts that encrypt $\pi_1, \ldots, \pi_t$, fully homomorphic encryption should allow anyone to output a ciphertext thet encrypts $f(\pi_1, \ldots, \pi_t)$ for any desired function f, as long as that function can be efficiently computed. No information about $\pi_1, \ldots, \pi_t$ or $f(\pi_1, \ldots, \pi_t)$, or any intermediate plain text values, should leak; the inputs, output and intermediate values are always encrypted.

Formally, there are different ways of defining what it means for the final ciphertext to "encrypt" $f(\pi_1, \ldots, \pi_t)$. The minimal requirement is correctness. A fully homomorphic encryption scheme ε should have an efficient algorithm Evaluate ε that, for nay valid ε key pairs (sk,pk), any circuit C, and any ciphertexts $\Psi_i \leftarrow Encrypt \; \varepsilon \; (pk, \pi_i)$, outputs

$\Psi \leftarrow Evaluate$ ε $(pk, C, \Psi_1, \ldots, \Psi_t)$, Such that Decrypt ε (sk,Ψ) = C$(\pi_1, \ldots, \pi_t)$.

B. THRESHOLD SECRET SHARING ALGORITHM

A threshold secret sharing scheme is defined by a probabilistic algorithm S. It takes as input a secret s chosen from some finite set S, and it outputs n shares, i.e., bit strings $s_1, \ldots, s_n$. Finally, the secret sharing scheme comes with a threshold t, a number with 0 $< t < n$. The idea is that if at most t shares are known, then this reveals nothing about s, whereas any set of at least $t + 1$ shares determine s uniquely. More precisely, we want:

Privacy: Take any subset I of the indices $\{1,2, \ldots, n\}$ of size at most t, and run S on input some $s \in S$. Then the probability distribution of $\{s_i | i \; \in I\}$ is independent of s.

Correctness: Take any subset J of the indices $\{1,2, \ldots, n\}$ of size at least $t + 1$, and run S on input some $s \in S$. Then s is uniquely determined by $\{s_i | i \; \in J\}$, and in fac there is an efficient algorithm that computes s from $\{s_i | i \; \in J\}$.

This concept was introduced by Shamir in 78, who also proposed the implementation we describe below. If we had such a scheme, we would use it to store one of the important keys we discussed earlier, by letting the key be the secret, and store the n shares in different locations. An adversary would have to get hold of at least $t + 1$ shares to steal the key, and on the other hand, as long as we loose no more than $n - t - 1$ shares, there will still be enough information to reconstruct the key. So this is a solution that is at the same time robust against loss of information and information leakage.

Assume we set $S = \mathbb{Z}_p$ for prime p, where $p > n$, and t is the threshold value we want. Then we can describe the algorithm S proposed by Shamir:

Choose elements $a_1, \ldots, a_t \in \mathbb{Z}_p$ at random, and let $f(x)$ be the polynomial$f(x) = s + \; a_1x + a_2x^2 + \cdots + a_tx^t$. In other words: choose a random polynomial $f(x)$ over $\mathbb{Z}_p$ of degree at most t, such that $f(0) = s$.

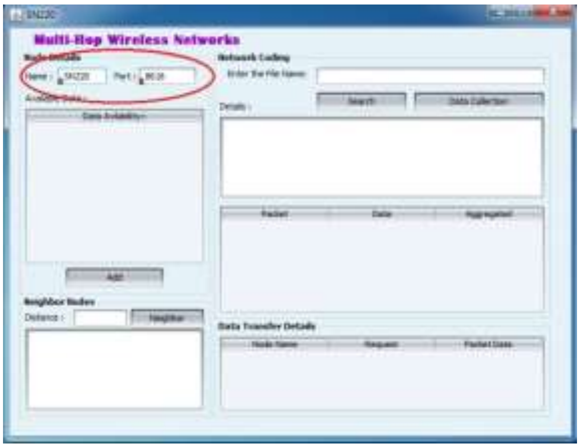
Let the shares be defined by $s_i = f(i)$mod p for $i = 1, \ldots, n$.

V. CONCLUSION

The improved form of novel network coding algorithm with homomorphic encryption algorithm and threshold secret sharing algorithm presented in this project is a solution to handle traffic analysis in multi-hop wireless network, which provides two significant privacy preserving features such as packet flow intractability and message content confidentiality, for efficiently thwarting the traffic analysis attack. Another feature of the project is that faster access of data from huge number of sensors in the network thus it reduces the energy consumption in the multi-hop wireless network.

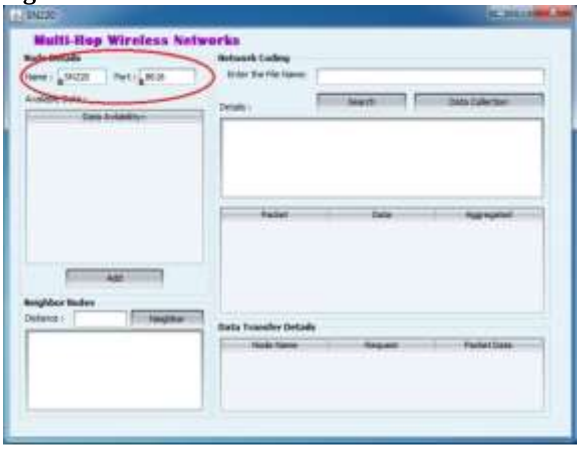
VI. FUTURE ENHANCEMENT

The quantitative analysis and simulative evaluation on privacy enhancement and computational overhead demonstrate the effectiveness and efficiency of the proposed scheme. In our future work, we will further improve the privacy preservation of the proposed scheme to achieve event source un observability by employing dummy messages



Name : SN220 Port : 8020

Fig A.2.1: Screenshot for Sensor Initialization



Name : SN220 Port : 8020

Fig A.2.1: Screenshot for Sensor Initialization

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe, and J.P. Smith, "Parametric Probabilistic Sensor Network Routing," Proc. ACM Int'l Conf. Wireless Sensor Networks and Applications (WSNA), pp. 122-131, 2003.

[3] M. Burmester and T.V. Le, "Secure Multipath Communication in Mobile Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, pp. 405-409, 2004.

[4] T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis, "Securing Wireless Sensor Networks Against Aggregator Compromises," IEEE Comm. Magazine, vol. 46, no. 4, pp. 134-141, Apr. 2008.

[5] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, C.E. Perkins, ed., pp. 139-172, Addison-Wesley, 2001.

[6] Y. Wu, P. A. Chou, and S.-Y. Kung, "Minimum-energy multicast inmobile ad hoc networks using network coding," *IEEE Trans. Commun.*,vol. 53, no. 11, pp. 1906-1918, Nov. 2005.

[7] P. A. Chou and Y. Wu, "Network coding for the Internet and wirelessnetworks," *IEEE Signal Process. Mag.*, vol. 24, no. 5, pp. 77-85, Sep.2007.

[8] Z. Li, B. Li, and L. C. Lau, "On achieving maximum multicast throughput in undirected networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2467-2485, June 2006.

[9] E. Ayday, F. Delgosha, and F. Fekri, "Location-aware security services for wireless sensor networks using network coding," in *Proc. IEEE INFOCOM '07*, pp. 1226-1234, 2007.

[10] M. Wang and B. Li, "Network coding in live peer-to-peer streaming,"*IEEE Trans. Multimedia*, vol. 9, no. 8, pp. 1554-1567, 2007.

[11] Fan, Y. Jiang, H. Zhu, and X. Shen, "An efficient privacy-preserving scheme against traffic analysis attacks in network coding," in *Proc. IEEE INFOCOM'09*, Rio de Janeiro, Brazil, Apr. 2009.

[12] V.Madhumitha,Dr.S.Kirubakaran, "A Survey on Anonymous Routing Protocols in Mobile Ad hoc Networks", International Journal of Computer Science Trends and Technology (IJCST) – Volume1 Issue2, Nov-Dec 2013.

[13]V.Oviya,Dr.S.Kirubakaran,K.Maheswari, "Enhancing Confidential Message Transferring System In A Security Framework" International Journal of Applied Engineering Research, ISSN 0973-4562 vol. 10 no.29 (2015).