International Journal of Scientific Research & Engineering Trends
Volume 3, Issue 5, Sept.-2017, ISSN (Online): 2395-566X

Encryption Scheme for Mobile Ad Hoc Networks: A Survey

Neha Dwivedi, Dr. Rajesh Shukla
Department of Computer Science & Engineering, SIRT, Bhopal
Email: dwivedi.neha001@gmail.com

***Abstract* – Network coding can help achieve lower energy consumption in MANETs. The energy saving comes from fact that less transmissions are required when in-network nodes are enabled to encode packets. We have to develop a new encryption scheme that can fully exploit the security property of network coding. Since both the coding vectors and message content are necessary for decoding, randomly reordering/mixing they will generate considerable confusion to the eavesdropping adversary. This paper gives a bird eye over light weighted authentications protocol.**

***Keywords* – MANET, Flooding AODV, P-code, Encryption Scheme, Battery Power.**

I. MOBILE AD-HOC NETWORK

A Mobile Ad-Hoc Network (MANET) is a temporary network having collection of wireless mobile nodes without using central access, infrastructure or centralized administration. There are number of characteristics in Mobile ad-hoc networks having verity of features, such as the dynamic network topology, limited bandwidth and energy constraint in the network. Mobile ad hoc network is significant for military operation to provide communication between squads, emergency case in out-of-the-way places, medical control etc. Routing in ad-networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility. A number of protocols have been developed for accomplish this task. Some of them are DSDV and AODV routing protocols. For communication nodes in the network should be able to sense and discover with nearby nodes. But transmission range of MANIT network interfaces is very limited; so for exchanging data within the node across the network may be required multiple network "hops" . One of the simple ways for routing is to send packets to the destination from the source node through intermediate nodes using the geometric information of all the nodes in the network. Getting accurate geometric information is still not easy. Where is one of another supplement of route determining by means of actively asking all the neighbours for information regarding shortest path to the destination.

The earliest broadcast mechanism is flooding [1], where every node in the network retransmits a message to all its neighbors upon receiving a message. Flooding is simple and easy to implement and it can be costly in terms of network performance, and one of the major problem that arise in flooding is "Broadcast Storm Problem". The broadcast storm problem results in high redundant message retransmissions, network bandwidth contention and collision. The flooding protocol have been studied [2] and its result indicates that rebroadcast could provide at most 61% additional coverage and only 41% additional coverage in average over that already covered by the previous broadcast. As a result, they have concluded that rebroadcasts are very costly and should be used with caution. To mitigate this problem, several broadcast schemes have been proposed [3,4, 5]. These schemes are commonly divided into two categories; deterministic schemes and probabilistic schemes. Deterministic schemes use network topological information to build a virtual backbone that covers all the nodes in the network. In order to build a virtual backbone, nodes exchange information, typically about their immediate or two hop neighbors. This results in a large overhead in terms of time and message complexity for building and maintaining the backbone, especially in the presence of mobility. Probabilistic schemes, in disparity, rebuild a backbone from scratch during each broadcast. Nodes make instantaneous local decisions about whether to broadcast a message or not using information derived only from overheard broadcast messages. These schemes incur a smaller overhead and demonstrate superior adaptability in changing environments when compared to deterministic schemes [6]. However, these schemes have poor reachability as a trade off against overhead. An optimal broadcast protocol minimizes, The maximum time needed for the broadcasted message to reach all nodes, The average time, over all the nodes, needed for the broadcasted message to arrive at each node.

Route establishment and maintenance overhead gradually increase in case of on-demand routing protocol. Whereas relative costs of these two components vary from one protocol to another. Whenever a route has to be discovered, the protocols have to perform some form of flooding of route request packets until the destination node is reached. Route maintenance involves re-establishment of a route, especially in the scenario of link failure or node failure.

A number of routing protocols using a variety of routing techniques have been proposed for use in MANETs. Adhoc On demand Distance Vector Routing (AODV) [9], Dynamic Source Routing (DSR) [10] , Temporally Ordered Routing Algorithm (TORA) [11], Location Aided

Routing (LAR) [12] (in which nodes search for or maintain a route only when route is needed), and periodic (proactive) protocols such as Destination Sequence Distance Vector (DSDV) [13], Distributed Bellman Ford [14] (in which nodes periodically exchange routing information and than can always know a current route to each destination). Also, several protocols use both reactive and proactive mechanism such as Zone Resolution Protocol (ZRP) [15], Cluster Based Routing Protocol (CBRP) [16]. The basic idea of on-demand routing protocols, is that a source node sends a route request and makes routing decision based on received route reply, which may be sent by destination or intermediate node. On-demand routing has several advantages, such as simplicity, correctness and flexibility. However, on-demand routing algorithms have the disadvantage of increasing per-packet overhead. This extra network overhead decreases the bandwidth available for transmission of data, increases the transmission latency of each packet, and consumes extra battery power in the network transmitter and receiver hardware. Due to manner of propagation route request (flooding), it is difficult to limit dissemination of unnecessary packets. The basic idea of proactive routing is periodically updating routing table via exchanging routing information. According to routing table, source node knows path or next hop to destination anytime when route needs. In proactive routing, route information is available when needed, resulting in little delay prior to data transmission. However proactive routing protocols are likewise not appropriate for mobile ad hoc networks, as they continuously use a large portion of the network capacity to keep the routing information current. Proactive routing protocols tend to distribute topological changes widely in the network, even though the creation/destruction of a new link at one end of the network may not be significant piece of information at the other end. The hybrid routing protocols pretends to inherit the best parts of both reactive and proactive routing protocols. The main idea of the hybrid routing protocols is the limiting the set of forwarding nodes and using the proactive routing algorithm for nearly placed nodes which usually forward data to far placed nodes. Network coding [11] can help achieve lower energy consumption in MANETs [6]–[8]. The energy saving comes from fact that less transmissions are required when in-network nodes are enabled to encode packets. We have to develop a new encryption scheme that can fully exploit the security property of network coding. Since both the coding vectors and message content are necessary for decoding, randomly reordering/mixing they will generate considerable confusion to the eavesdropping adversary.

II. CURRENT SCENARIO

Ren Yueqing [6]design and construction of wireless sensor networks. A desirable topology can extend the lifetime of the entire network. This paper focuses on the complexity of the structure of the topology of wireless sensor network and analyze their complex characteristics in terms of the theory of network science. This is beneficial for improving the efficiency of energy use of the network.

Bala Krishna [7]propose Energy organized aware clustering protocol (SECC) for sensor networks wireless sensor network group based energy node and groups of remote nodes. If the energy of the node is less than the threshold value, SECC self-organized clusters of forms and reorganize the sensor array. The nodes having less than the threshold value energy attributes are removed from the cluster network to maintain efficient energy sensors. Energy management in clusters SECC node function parameters (such as remote node, power node, the node density) and cluster parameters (such as cluster density, sensor nodes per group).

Boniewicz8]proposed in the method of the wireless sensor network is compared. Energy consumption is very important for self-powered radio nodes. But some energy applications balance is more important. Networks of wireless sensors used in large areas such as farmland or stores consist of hundreds of nodes. In the conventional method of routing is directed to transmit a short time and low energy consumption. But consumption of unbalanced energy can often cause unpredictable failures due to lack of energy in the nodes of frequent use. Energy balance to avoid this dynamic behavior by skipping nodes used. The document discloses examples of algorithms that may be used in the method of the wireless sensor network. The aim of this method is the extension of the network via a data path selection to minimize the dispersion of energy in the network nodes.

Baghyalakshmi [10]present a study of routing protocols low latency critical and time efficient energy. TEEN (network protocol the threshold energy efficient Light Sensor), reactive network protocol that is well suited for the detection of data time-critical applications is very efficient in terms of energy consumption and response time . APTEEN (network protocol energy efficient sensors for periodic adjustment of the sensitivity threshold), a protocol for hybrid network which gives the overall picture of the network at regular intervals so very effective energy. Speed is a stateless protocol, highly efficient and scalable sensor networks reaching end to end communication in soft real-time, maintaining a desired delivery rate of the network with a new combination of control feedback and geographic non-deterministic transmission. RAP, a communication architecture for sensor networks in real-time scale significantly reducing latency to stop using the top speed - monotonous programming (VMS). APRN, current power routing protocol that supports real-time energy efficiency real-time communication by dynamically adapting transmission power and routing decisions. The advantages and performance issues of each routing protocol are also discussed.

Peng Zhang11]Propose P-Coding, a lightweight encryption scheme to provide confidentiality for network-

coded manets in an energy-efficient way. The basic idea of P-Coding is to let the source randomly permutes the symbols of each packet (which is prefixed with its coding vector), before performing network coding operations. Without knowing the permutation, eavesdroppers cannot locate coding vectors for correct decoding, and thus cannot obtain any meaningful information.

Applying P-Coding in these applications are not as high as in MANETs, since these applications are generally not energy-constrained and any symmetric cryptographic algorithms would function well. We will extend our scheme to other scenarios where encryption efficiency is critical.. The objective of this dissertation is to develop a new approach which can successfully maintain the confidentiality with lesser battery power in order to long survival of mobile ad-hoc network.

III. CONCLUSION

This paper studied the problem of energy saving in MANETs based on the technique of network coding. Previous studies demonstrated that network coding can reduce energy consumption with less transmission in MANETs. We proposed optimized P-Coding, a lightweight scheme on top of network coding, to further reduce energy consumption in MANETs by cutting the security cost. We will showed that optimized P-Coding is efficient in computation, and incurs less energy consumption for encryptions/decryptions.

REFERENCES

[1] ZunnunNarmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[2] Sheikh, R. , Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review", IEEE 2010, pp 1-4.

[3] Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., " A survey of routing attacks in mobile ad hoc networks" IEEE 2007, pp 85-91.

[4] Verma, M.K. and Joshi, S. ; Doohan, N.V. "A survey on: An analysis of secure routing of volatile nodes in MANET", IEEE 2012, pp 1-3.

[5] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[6] Ren Yueqing , Xu Lixin A study on topological characteristics of wireless sensor network based on complex network", IEEE 2010, pp 486 - 489

[7] Bala Krishna, M., Doja, M.N., "Self-organized energy conscious clustering protocol for wireless sensor networks", IEEE 2012,pp 521 - 526

[8] Boniewicz, Miroslaw Toruń, Poland Kozlowska, Anna ; Zawadzka, Anna ; Lukasiak, Zbigniew ; Zielinski, Marek "Review of selected algorithms in the method energy evening algorithm in wireless sensor network", IEEE 2014, pp 1 – 4.

[9] Hartwell, R., Wireless Sensor Network Energy Use While Tracking Secure Area Intrusions" IEEE 2013, pp 1696 – 1701

[10] Baghyalakshmi, D. ; Ebenezer, J. ; SatyaMurty, S.A.V. "Low latency and energy efficient routing protocols for wireless sensor networks", IEEE 2010, pp 1 – 6.

[11] Peng Zhang, Chuang Lin "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks" in IEEE Transactions on Parallel And Distributed Systems, 1045-9219, 2013 IEEE[11]