International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 2 – FEBRUARY 2016.

ENHANCED HYBRID WIRELESS NETWORK FOR DISTRIBUTED THREE-HOP ROUTING PROTOCOL WITH HOMOMORPHIC ENCRYPTION ALGORITHM

[1] Mrs.T.Sathya Priya[2] V.Bhuvaneswari

M.Sc.,M.Phil., Department of Computer Science, Theivanai Ammal College for Women (Autonomous), Villupuram-605 401.
M. Phil Scholar(Computer Science), Theivanai Ammal College for Women (Autonomous), Villupuram-605 401.

Sathyakumar141@gmail.com
bhuvi.reach89@gmail.com

***Abstract-* Due to the increasing level of wireless communication in today's environment, people often requires distributed environment for sharing their data between the nodes. For affording an effective communication to the user, many researchers proposed a very few methods to provide three-hop routing protocol that guaranteed routing for hybrid networks, they strive to improve the network capacity and reliability but they evade constrain in securing the data. For this problem, our main objective of this paper is to improve the effective and efficiency of routing approach with constrains over hybrid wireless data streaming using Distributed Three-hop routing protocols and Homomorphic Encryption algorithm. This aims to develop the secure based reliable architecture against the hybrid wireless routing issues. The system also aims at providing both proactive and reactive solutions for effective routing. The goal of this paper is to providing efficient dynamic routing management to deal the challenges of data transmission and data streaming in hybrid mobile environments.**

Keywords- Hybrid Wireless Network, Distributed Three-hop routing protocols, Homomorphic Encryption algorithm and reliable architecture.

I. INTRODUCTION

WIRELESS access networks, 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. Multi-hop Wireless Networks (MWNs) are regarded as a highly promising solution for extending the radio coverage range of the existing wireless networks, and they can also be used to improve the system reliability through multi-path packet forwarding. However, 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. 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.

It is very challenging to efficiently thwart traffic analysis/flow tracing attacks and provide privacy protection in MWNs. Existing privacy-preserving solutions, such as proxy based schemes [3], [4], Chaum's mix-based schemes [5], [6], and onion-based schemes [7], [8], may either require a series of trusted forwarding proxies or result in severe performance degradation in practice. Different from previous schemes, our research investigates the privacy issue from a brand new perspective: using network coding to achieve privacy preservation.

II. RELATED WORK

Network coding was first introduced by Ahlswede et al [9]. Subsequently, two key techniques, random coding [10] and linear coding [11], [12] ([12] gives the first distributed implementation), further promoted the development of network coding. The random coding makes network coding more practical, while the linear coding is proven to be sufficient and computationally efficient for network coding. Currently, network coding has been widely recognized as a promising information dissemination approach to improve network performance. Primary applications of network coding include file distribution and multimedia streaming on P2P overlay networks [13], data transmission in sensor networks [14], tactical communications in military networks [15], etc. Compared with conventional packet forwarding technologies, network coding offers, by allowing and encouraging coding/mixing operations at intermediate forwarders [9], several significant advantages such as potential throughput improvement [16], transmission energy minimization [17], and delay reduction [18]. In addition, network coding can work as erasure codes to enhance the dependability of a distributed data storage system [19]-[22].

The deployment of network coding in MWNs can not only bring the above performance benefits, but also provide a feasible way to efficiently thwart the traffic analysis/flow tracing attacks since the coding/mixing operation is encouraged at intermediate nodes. Similar to Chaum's mix-based schemes [5], [6], network coding provides an intrinsic message mixing mechanism, which implies that privacy preservation may be efficiently achieved in a distributed manner [23]. Moreover, the unlinkability between incoming packets and outgoing packets, which is an important privacy property for preventing traffic analysis/flow tracing, can be achieved by mixing the incoming packets at intermediate nodes. However, the privacy offered by such a mixing feature is still vulnerable, since the linear dependence between outgoing and incoming packets can be easily analyzed. A simple deployment of network coding cannot prevent traffic analysis/flow tracing since the explicit Global Encoding Vectors (GEVs, also known as tags) prefixed to the encoded messages provide a back door for adversaries to compromise the privacy of users. Once enough coded packets are collected, adversaries can easily recover the original packets and then conduct the attacks based on these packets. A naive solution to address this vulnerability is to employ link-to-link encryption. This solution can prevent traffic analysis to a certain degree, but it introduces heavy computational overhead and thus results in significant performance degradation of the whole network system. Additionally, it cannot protect the privacy of users once some intermediate nodes are compromised by adversaries. Such deficiencies motivate us to explore an efficient privacy-preserving scheme for Mobile Wireless Networks.

III. HYBRIDIZED HOMOMORPHIC ENCRYPTION ALGORITHM WITH 3-HOP ROUTING

This section describes about the hybridized homomorphic encryption algorithm in distributed manner. Distributed Three-hop Routing Protocol is an improved routing protocol where a source node segments the messages into different streams into a number of segments. Each segmented data is forwarded to its neighbor node in mobile networks. The relay nodes are communicated either through direct or relay transmission to the Base Station. The segmented data is forwarded to its neighbor nodes with higher capacity to Base Station in relay transmission. In direct transmission, a segment is directly forwarded to a BS. In the infrastructure, the segments are rearranged in their original order and sent to the destination. The number of routing hops in DTR is confined to three, including at most two hops in the ad-hoc transmission mode and one hop in the cellular transmission mode. It works in three phases. The first phase is to balance the nodes, second phase is to design the routing protocols for data, third phase is to develop a multiplane clos- network and fourth phase is to develop a homomorphic encryption algorithm.

i) Load Balancing

An intermediate node forwards the packet with the first smallest amount time allowed to forwarded the resolute succeed fairness in packet forwarding. An intermediate node forwards the packets in the order from the packets with the closest deadlines to the packets with the farthest deadlines. If an intermediate node has no problem to meet all packets' deadlines in forwarding, that is, the packets are scheduling feasible, the load balancing works effectively.

ii) Data Routing Protocols

Data Routing Protocols works as Buffer Management. The packets are queued in the buffer management systems. The output scheduler gets packets to output the information. A multiplexer is used for the intra-flow packets.

iii) Wireless Network

In a multi-plane multi-path switch, cells may travel through different paths and experience different queuing delays. Thus, packets can be delivered out-of-sequence through the switch fabric. To maintain packet order in the Buffer switch, we studied four port-to-port flow control schemes. They can be categorized into two approaches namely hashing method and buffer resequencing method. In the first approach, hashing, we force the cells belonging to the same flow to take the same path through the switch. As a result, all cells from a given flow will experience the same amount of queuing delay. Thus packets are delivered in order. Along this approach, they presented two hashing schemes: static hashing and dynamic hashing. On the other hand, the buffer resequencing approach allows packet out-of-sequence within the switch fabric. However, TME uses a resequencing buffer to resequence the cells back in order before delivering them to the next link. It is a time-stamp-based resequencing and window-based resequencing.

iv) Homomorphic Encryption Algorithm

Homomorphic Encryption Algorithm works as follows:

i) KeyGen: Let λ be a security parameter that outputs Secret key S_k and public key P_k.

ii) Encryption: The input is given as plaintext $\pi \in \{0,1\}$ and Pk. Then the cipher text φ

iii) Decryption: Using the ciphertext φ and secret key Sk, returns plaintext π .

iv) Steps: Based on t-input circuit C and tuple of cipher texts, the modulo operation executes and returns the Ciphertext φ .

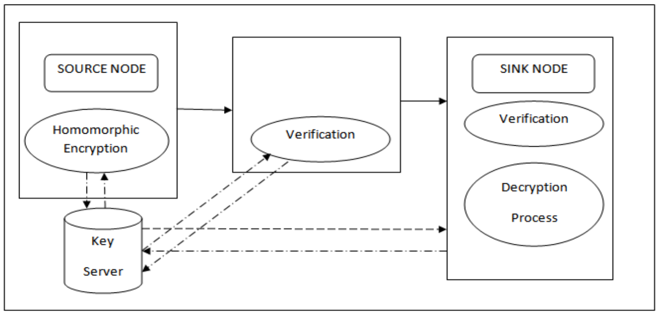

Fig.1. Proposed Architecture

IV. EXPERIMENTAL RESULTS

The experimental result shows the difference between the existing and the proposed architecture for providing the better result for the Distributed Three Hop routing protocol in Hybrid network. The performance metrics Packet Rate Vs Storage time limit is executed and shown in Fig. 2. Three hops are utilized for information transmission as a part of a system. Two hops at mobile Adhoc system and one hop at the infrastructure system. The use of this merged combination will enhance the unwavering quality. In this strategy, the system is noiseless until an association is required. Alternate node sent this message and documentation the nodes that they heard it from, making a blast of interim courses is back to the required hub. At the point, when a hub gets such a message, it will send the message in reverse through an interim course to the requested hub. The denied hub then starts utilizing the course that is minimal number of hops through different hubs. Idled nodes in the steering tables are reused after a period. The advantages of the proposed approach were listed as follows:

DTR significantly increases the throughput capacity and scalability of hybrid wireless networks by overcoming the three shortcomings of the previous routing algorithms. It has the following features:

i) Low overhead: In the dynamic environment, it eliminates overhead caused by route discovery and maintenance in the ad-hoc transmission mode.

ii) Hot spot reduction: It alleviates traffic congestion at mobile gateway nodes while makes full use of channel resources through a distributed multi-path relay.

iii) High reliability: Because of its small hop path length with a short physical distance in each step, it alleviates noise and neighbor interference and avoids the adverse effect of route breakdown during data transmission. Thus, it lessen the packet drop rate and makes full use of spatial reuse, in which several source and destination nodes can communicate simultaneously without any interference.

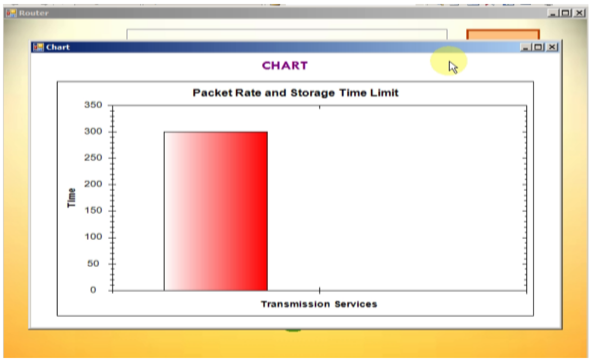

Fig.2. Packet Rate Vs Storage Time limit

V. CONCLUSION

This paper proposed an efficient secure distributed homomorphic encryption algorithm that addresses some issues specific to Hybrid wireless networks which are communication delay, cost, mobility, and link unreliability. Nodes fasten the details about the forwarding nodes in the packet header. This also creates a virtual node for effective data transmission. The system implements an appropriate scheme which is named as Homomorphic Encryption Algorithm for mobility analysis during transmission. This helps to find closest neighbor already in the group therefore reducing the cost of join requests broadcast and reducing the communication and computation cost incurred by the source. The concentration on selective congestion attacks by applying effective traffic and node monitoring techniques. The priority based traffic allocation with effective technique will be considered more in future.

REFERENCES

[1] H Luo, R. Ramjee, P. Sinha, L. Li, and S. Lu. Ucan: A unified cell and ad-hoc network architecture. In Proc. of MOBICOM, 2003.

[2] P. K. McKinley, H. Xu, A. H. Esfahanian, and L. M. Ni. Unicastbased multicast communication in wormhole-routed direct networks. TPDS, 1992.

[3] H. Wu, C. Qiao, S. De, and O. Tonguz. Integrated cell and ad hoc relaying systems: iCAR. J-SAC, 2001.

[4] Y. H. Tam, H. S. Hassanein, S. G. Akl, and R. Benkoczi. Optimal multi-hop cellular architecture for wireless communications. In Proc. of LCN, 2006.

[5] Y. D. Lin and Y. C. Hsu. Multi-hop cellular: A new architecture for wireless communications. In Proc. of INFOCOM, 2000.

[6] P. T. Oliver, Dousse, and M. Hasler. Connectivity in ad hoc and hybrid networks. In Proc. of INFOCOM, 2002.

[7] E. P. Charles and P. Bhagwat. Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers. In Proc. of SIGCOMM, 1994.

[8] C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc on demand distance vector (AODV) routing. Technical report, Internet Engineering Task Force, 2003.

[9] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. IEEE Mobile Computing, 1996.

[10] V. D. Park and M. Scott Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In Proc. Of INFOCOM, 1997.

[11] R. S. Chang, W. Y. Chen, and Y. F. Wen. Hybrid wireless network protocols. IEEE Transaction on Vehicular Technology, 2003.

[12] G. N. Aggelou and R. Tafazolli. On the relaying capacity of next generation gsm cellular networks. IEEE Personal Communications Magazine, 2001.

[13] T. Rouse, I. Band, and S. McLaughlin. Capacity and power investigation of opportunity driven multiple access (ODMA) networks in TDD-CDMA based systems. In Proc. of ICC, 2002.

[14] H. Y. Hsieh and R. Sivakumar. On Using the Ad-hoc Network Model in Wireless Packet Data Networks. In Proc. of MOBIHOC, 2002.

[15] L. M. Feeney, B. Cetin, D. Hollos, M. Kubisch, S. Mengesha, and H. Karl. Multi-rate relaying for performance improvement in ieee 802.11 wlans. In Proc. of WWIC, 2007.

[16] Haiying Shen, Ze Li and Chenxi Qiu, "A Distributed Three-hop Routing Protocol to Increase the Capacity of Hybrid Wireless Networks", IEEE Transactions on Mobile Computing , 2015.