*Impact Factor (SJIF): 4.542*

**International Journal of Advance Research in Engineering, Science & Technology**

*e-ISSN: 2393-9877, p-ISSN: 2394-2444*

***Volume 4, Issue 12, December-2017***

# Privacy management in wireless ad-hoc network using multihop communication

**Manali Nivalkar[1], Sneha Patil[2], Rinkal Raut[3], Varsha Jagadale[4], Dr S.T Singh[5],**

**Prof. T. R. Salunkhe[6]**

***[1,2,3,4,5,6]P.K. Technical Campus, Computer Engineering, Chakan, Pune.***

manumanali7111@gmail.com

rinkalraut97@gmail.com

sp928935@gmail.com

varsha6jagadale@gmail.com

pteju147@gmail.com

**Abstract---** During this paper, system proposes a unique light-weight theme to effectively transmit information from supply to destination. In projected for information secret writing system target the AES algorithmic program. The projected system introduces economical mechanisms for information verification and reconstruction at the base station (Destination). Additionally, the system extends the secure information theme with practicality to sight packet drop attacks staged by malicious information forwarding nodes. System valuate the projected technique each analytically and by trial and error, and also the results prove the effectiveness and potency of the light-weight secure information theme in police work packet forgery, loss attacks and alter destination through hacker.

**Keywords:** Packet Drop, AES algorithm, Confidentiality.

## I. INTRODUCTION

Wireless networks are getting more and more standard in varied application domains, like cyber physical infrastructure systems, environmental observance, power grids, etc. information area unit made at an oversized range of wireless node sources and processed in-network at intermediate hops on their thanks to a base station that performs decision-making.

The diversity of knowledge sources creates the necessity to assure the trustiness of knowledge; specified solely trustworthy data is taken into account within the call method. Information is a good technique to assess information trustiness, since it summarizes the history of possession and therefore the actions performed on the info.

Large-scale wireless networks area unit deployed in varied application domains, and therefore the information they collect area unit employed in deciding for essential infrastructures. System thinks about the matter of resource allocation and management of multihop networks [1] during which multiple source-destination pairs communicate confidential messages, to be unbroken confidential from the intermediate nodes. System proposes the matter as that of network utility maximization, into that confidentiality is incorporated as an extra quality of service constraint. Information area unit streamed from multiple sources through intermediate process nodes that mixture data.

## II. RELATED WORK

In Secure Distributed Information Exchange [2] considers the problem of streaming a file by exchanging information over wireless channels in the presence of an eavesdropper. We utilize private and public channels and wish to minimize the use of the (more expensive) private channel subject to a required level of security. Here authors consider both single & many users and compare easy ARQ and deterministic network coding as methods of transmission. In Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel [3] characterize the secrecy capacity in terms of generalized eigenvalues when the sender and eavesdropper have multiple antennas, the intended receiver has a single antenna, and the channel matrices are fixed and known to all the terminals, and show that a beam forming strategy is capacity-achieving. In Data Confidentiality in Mobile Ad hoc Networks [4] Mobile ad hoc networks (MANETs) are self-configuring infrastructure-less networks comprised of mobile nodes that communicate over wireless links without any central control on a peer-to-peer basis. These individual nodes act as routers to forward both their own data and also their neighbor's data by sending and receiving packets to and from other nodes in the network. It's a relatively very easy configuration and the quick deployment makes ad hoc networks appropriate the emergency conditions. In Control of Wireless Networks with Secrecy [5] here it take into consideration the problem of cross-layer resource allocation with time-varying cellular wireless networks, and incorporate information theoretic secrecy like a Service quality constraint. Specifically, each node within the network injects 2 types of traffic, private and open, at rates chosen as a way to maximize an international utility function, susceptible to network stability and secrecy constraints. Secrecy limitation enforces a randomly small mutual info leakage in the source to each and every node inside the network, apart from the sink node.

## III. EXISTING SYSTEM

In existing system, confidentiality of communicated information between the nodes is necessary but the existing system not cable to shared information to any other node. So they are not providing any confidentiality regarding to the message. Even in scenarios in which confidentiality is not necessary; it may be dangerous to assume that nodes will always remain uncompromised. Keeping different nodes' information confidential can be viewed as a precaution to avoid a captured node from gaining access to information from other un-captured nodes.

### 3.1 Disadvantages of Existing System

1. Network performance becomes low.
2. The confidentially regarding message not intended.
3. Recovery of data is not possible.

## IV. PROPOSED SYSTEM

In this paper, system considers wireless networks in which messages are carried between the source destination pairs cooperatively in a multi-hop fashion via intermediate nodes. In a multihop network, as data packets are transferred, intermediate nodes obtain all or part of the information through directly forwarding data packets or overhearing the transmission of nearby nodes. This poses a clear problem when transferring confidential messages. In this paper, system builds efficient algorithms for confidential multiuser communication over multihop wireless networks without the source-destination pairs having to share any secret message.

Our goal is to design an efficient encoding and decoding mechanism that satisfies such security and performance needs. System proposes an encoding strategy whereby each node on the path of a data packet securely embeds information within an AES algorithm that is transmitted along with the data. Upon receiving the packet, the destination extracts and verifies the data information. We also devise an extension of the data encoding scheme that allows the BS (Destination) to detect if a packet drop attack was staged by a malicious node. To detect if destination change was staged by a malicious node.

### 4.1 Advantages of Proposed System

1. We formulate the problem of secure data transmission in wireless networks, and identify the challenges specific to this context.
2. We propose an AES algorithm for data encoding and data decoding scheme.
3. We design efficient techniques for data decoding and verification at the base station (Destination).
4. We extend the secure data encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious node.

## V. SYSTEM ARCHITECTURE

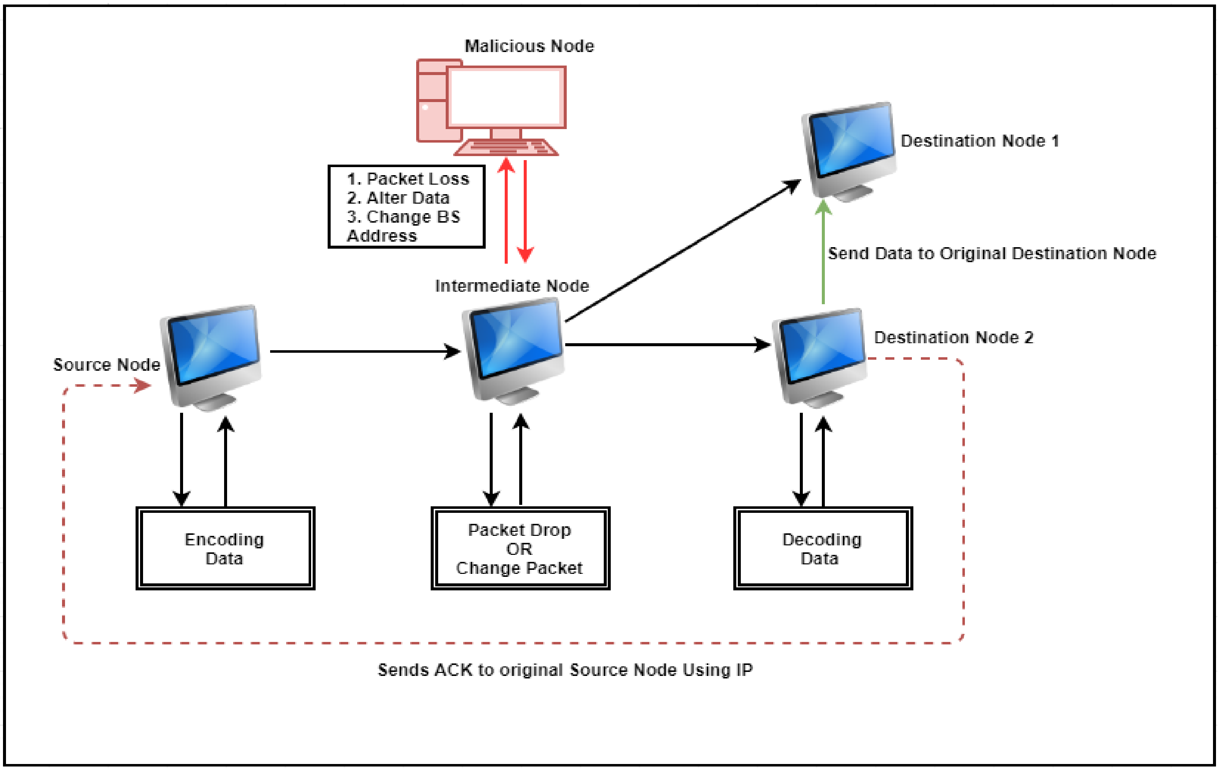

***Figure 1. Proposed System Architecture***

## VI. CONCLUSION

In this paper, we considered the problem of resource allocation in wireless multi-hop networks where sources have confidential information to be transmitted to their corresponding destinations with the help of intermediate nodes. All intermediate nodes are considered as internal eavesdroppers from which the confidential information needs to be protected. To provide confidentiality in such setting, we propose encoding the message over long blocks of information which are transmitted over different paths. Then, we designed a dynamic control algorithm for a given encoding rate and we prove that our algorithm achieves utility arbitrarily close to the maximum achievable utility.

## REFERENCES

[1] Sarikaya, Yunus, C. Emre Koksal, and Ozgur Ercetin. "Dynamic network control for confidential multi-hop communications." IEEE/ACM Transactions on Networking (TON) 24.2 (2016): 1181-1195.

[2] Abuzainab, Nof, and Anthony Ephremides. "Secure distributed information exchange." *IEEE Transactions on Information Theory* 60.2 (2014): 1126-1135.

[3] Khisti, Ashish, and Gregory W. Wornell. "Secure transmission with multiple antennas I: The MISOME wiretap channel." *IEEE Transactions on Information Theory* 56.7 (2010): 3088-3104.

[4] Aldabbas, Hamza, et al. "Data confidentiality in mobile ad hoc networks." *arXiv preprint arXiv:1203.1749* (2012).

[5] Koksal, C. Emre, Ozgur Ercetin, and Yunus Sarikaya. "Control of wireless networks with secrecy." *IEEE/ACM Transactions on Networking (TON)* 21.1 (2013): 324-337.