International Journal of Advance Research in Engineering, Science & Technology

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

Volume 4, Issue 12, December-2017

Achieving Confidentiality in Wireless Network using Dynamic Control Algorithm

Anurupa Mitra[1], Supriya Kajale[2], Rushikesh Shinde[3], Prof. Manisha Bharati[4]

Student, Department of Computer Engineering, Indira College of Engineering and Management, Pune, India

***Abstract*-- Large-scale ad-hoc networks are deployed in numerous application domains, and the data they collect are used in decision making for critical infrastructures. We consider the problem of resource allocation and control of multi-hop networks in which multiple source-destination pairs communicate confidential messages, to be kept confidential from the intermediate nodes. We act the problem as that of network service maximization, into which confidentiality is incorporated as an additional quality of service constraint. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. In this paper, we propose a novel lightweight scheme to securely transmit data. The proposed technique relies on in-packet Bloom filters to encode data. We introduce efficient mechanisms for data verification and reconstruction at the base station. In addition, we extend the secure data scheme with process to detect packet drop attacks execute by malicious data forwarding nodes. We classify the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure data scheme in detecting packet forgery and loss attacks.**

***Keywords*-- Packet Drop, Bloom Filter, Lightweight, Packet Forgery Confidentiality.**

I. INTRODUCTION

Sensor networks are becoming increasingly popular in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc.

Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. We investigate the problem of secure and efficient data transmission and processing for sensor networks. In a multi-hop sensor network, data verification allows the base station to trace the source and forwarding path of an individual data packet since its generation. Verification must be recorded for each data packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of the sensor nodes. Therefore, it is necessary to devise a light-weight solution which does not introduce significant overhead. Furthermore, sensors often operate in an untrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. Our goal is to design a data encoding and decoding mechanism that satisfies such security and performance needs. We propose a data encoding strategy whereby each node on the path of a data packet securely embeds verification information within a Bloom filter, which is transmitted along with the data. Upon receiving the data, the base station extracts and verifies the data. In existing system, confidentiality of communicated information between the nodes is necessary but the existing system not able to share 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. Hence to overcome some drawbacks like to detect if destination change was staged by a malicious node, the confidentially regarding message not intended and recovery of data is not possible.

In this paper our main objectives are Data should be decoded only at destination node as to achieve confidentiality, Integrity is maintained as adversary cannot add or remove data from node and Freshness: An adversary cannot replay captured data and data without being detected by the BS (Destination) due to this we consider wireless networks in which messages are carried between the source destination pairs cooperatively in a multi-hop fashion

via intermediate nodes. In a multi hop 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. System builds efficient algorithms for confidential multiuser communication over multi hop 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 a RSA 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 Base Station (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. Therefore we formulate the problem of secure data transmission in wireless networks, and identify the challenges specific to this context.

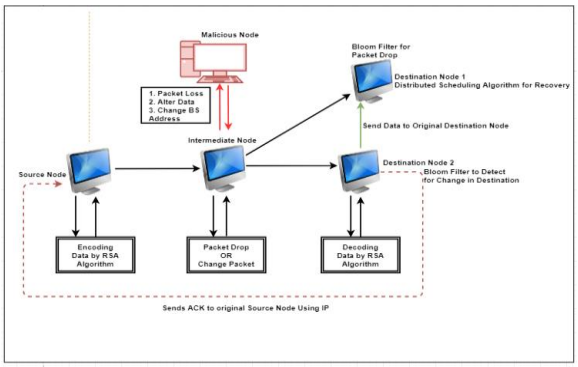
We propose a RSA algorithm for data encoding and data decoding scheme. We design efficient techniques for data decoding and verification at the base station (Destination). We extend the secure data encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious node. We perform a detailed security analysis and performance evaluations of the proposed data encoding scheme and packet loss, packet alter detection mechanism with destination change.

II. RELATED MODEL

In the multihop setting, studies the secrecy capacity scaling problem. Exploitation of path diversity in order to achieve secrecy from external eavesdroppers is studied in and for secrecy via mobility. In a method is given that modifies any given linear network code into a new code that is secure requiring a large field size. Later, generalized and simplified the method, and showed that the problem of making a linear network code secure is equivalent to the problem of finding a linear code with certain generalized distance properties. Along the same lines, investigates secure communication over wireless networks where a node can observe one of an arbitrarily selected collection of secure link sets. In, a different notion of security referred to as packet-level security is used, where it is sufficient that the eavesdropper does not correctly decode the message, i.e., it does not guarantee full equivocation.
Recently in, we have investigated the cross-layer resource allocation problem with confidentiality in a cellular wireless network, where users transmit information to the base station, confidentially from the other users. In this paper, we consider a general multi-hop network topology and develop dynamic network control algorithms to jointly determine the end-to-end encoding rates, scheduling and routing.

III. SYSTEM MODEL

Each source node in aims to keep its information confidential from the nodes in the set of. To that end, a source node precodes its message, divides it into multiple pieces, and sends separate pieces over different paths to the destination. Henceforth, none of the intermediate relay nodes in the set of will accumulate sufficient amount of information to decode the confidential message, even in part.



In a multi-hop sensor network, the origin of data allows the BS to trace the source and forwarding path of an individual data packet. Origin must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes. Therefore, it is necessary to devise a solution with low overhead. The sender (source) will send the message i.e. data packets by data encoding scheme and send to

destination via intermediate nodes. Our system detects automatic packet drop (by low bandwidth, frequency, etc factors), or packet drop by hacker, with the help of bloom filter.

IV. ATTACKER MODEL

Each attacker is capable of tapping into all the information transmitted and received by a single intermediate node. Attackers are not capable of changing the content of the information the node forwards, nor do they inject phantom messages into the network. In our model, intermediate nodes are entities, compliant with network operations as they properly execute algorithms, but the messages need to be kept confidential from them. The main additional challenges involved in generalizing problem to multihop networks are Dynamic end-to-end encoding and multipath routing. Standard dynamic control algorithms give control decisions in each time slot independently by assuming time-scale separation, i.e., independent transmissions of subsequent slots. The confidential message is encoded across many blocks, which implies that the time-scale involved in physical-layer resource allocation cannot be decomposed from the time scales involved in network-layer resource allocation, eliminating the time-scale separation assumption of standard dynamic control algorithms.

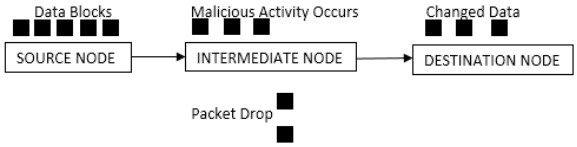


Fig 1. Packet Drop Attack

Packet Drop Attack is also known as Blackhole attack or Greyhole attack. Here a compromised node drops packet maliciously. Several techniques have been proposed to detect the packet drop attack in wireless networks. Therefore in this paper we review some of the packet drop attack detection techniques by using Bloom Filter and recovery of packets is done by using distributed scheduling algorithms.

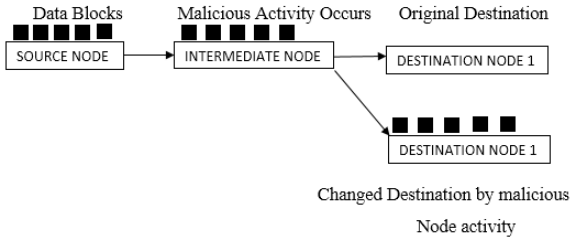


Fig 2. Change in Destination Attack

Similarly Change in Destination attack can also be detected by using Bloom Filter, therefore by sending acknowledgement to source we can identify the correct destination.

V. ALGORITHM & TECHNIQUE

We propose a dynamic control algorithm associate with end-to-end secrecy encoding, where messages are encoded over infinitely many blocks. Hence, the decoding delay of confidential message may be infinitely long. Unlike the infinite-block case, since a message is encoded across a finite number of blocks, subsequent packets associated with a given secrecy encoded message cannot be decoupled. Therefore, achieving perfect secrecy for all messages is not possible. Hence, we define the notion of secrecy outage. We say that a secrecy outage event occurs, when the confidential message is intercepted by any intermediate node, i.e., the perfect secrecy constraint is violated.

1. *Dynamic Control Algorithm and Techniques*

A. Control Technique 1: Sequence Number

Scenario 1:

First source node will send file to destination then here the sequence number generated as 1.Then the file will pass through intermediate node then the sequence number generated as 2. Finally reaches at destination address. The destination checks the sequence number. It shows that the sequence number is finally 2. Then destination will get that the data which node received is accurately without change in data.

Scenario 2:

First source node will send file to destination then here the sequence number generated as 1.Then the file will pass through intermediate node then the sequence number generated as 2. When data reaches at intermediate node then hacker will drop the data, alter the data or change the destination address then the sequence number generated as 3. Destination node received the data with 3 sequence number. Then destination will get the information that node received the data by 3 sequence number then the node received the data with extra sequence number. Then it will get the information that the malicious node changes the data.

B. Control Algorithm 1: RSA Algorithm

RSA encrypts messages through the following algorithm, which is divided into 3 steps:

1. Key Generation

I. Choose two distinct prime numbers p & q.

II. Find n such that n = pq. n will be used as the modulus for both the public and private keys.

III. Find the totient of n, $\phi(n)$

$\phi(n)=(p-1)(q-1)$.

IV. Choose an e such that $1 < e < \phi(n)$, and such that e and $\phi(n)$ share no divisors other than 1 (e and $\phi(n)$ are relatively prime) e is kept as the public key exponent.

V. Determine d (using modular arithmetic) which satisfies the congruence relation

$de \equiv 1 \pmod{\phi(n)}$.

In other words, pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or $\phi(n)$. This is often computed using the Extended Euclidean Algorithm, since e and $\phi(n)$ are relatively prime and d is to be the modular multiplicative inverse of e. d is kept as the private key exponent. The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

2. Encryption

I. Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.

II. When Person B wishes to send the message "M" to Person A, he first converts M to an integer such that $0 < m < n$ by using agreed upon reversible protocol known as a padding scheme.

III. Person B computes, with Person A's public key information, the ciphertext c corresponding to

$c \equiv m^e \pmod{n}$.

IV. Person B now sends message "M" in ciphertext, or c, to Person A.

3. Decryption

I. Person A recovers m from c by using his/her private key exponent, d, by the computation

$m \equiv c^d \pmod{n}$.

II. Given m, Person A can recover the original message "M" by reversing the padding scheme. This procedure works since

$c \equiv m^e \pmod{n}$,

$c^d \equiv (m^e)^d \pmod{n}$,

$c^d \equiv m^{de} \pmod{n}$.

By the symmetry property of mods we have that $mde \equiv mde \pmod{n}$. Since $de = 1 + k\phi(n)$, we can write

$mde \equiv m1 + k\phi(n) \pmod{n}$,

$mde \equiv m(mk)\phi(n) \pmod{n}$,

$mde \equiv m \pmod{n}$.

From Euler's Theorem and the Chinese Remainder Theorem, we can show that this is true for all m and the original message

$cd \equiv m \pmod{n}$, is obtained.

C. Control Algorithm

2: Distributed Scheduling Algorithm

Each node carries out the following steps over each block:

Calculate size file which will be is send to nodes. Send a file to destination node. If the request will be change by the intermediate node to another destination then node will check for matching request and send file to original destination. Otherwise node sends ACK to original source node using IP. After receiving a matching request from another destination address then node checks the received request. Upon receiving ACK from another destination to source node then it will checked for matching request. If both nodes check the request then they will transmit the data and get the information that data is changed by malicious node.

2. Bloom Filter

Bloom filters are compact data structures for probabilistic representation of a set in order to support membership queries (i.e. queries that ask: "Is element X in set Y?"). This compact representation is the payoff for allowing a small rate of false positives in membership queries; that is, queries might incorrectly recognize an element as member of the set.

```
Procedure BloomFilter(setA,hash_functions, integer m)
        returns filter
  filter = allocate m bits initialized to 0
  foreach ai  in A:
                foreach hash function hj:
      filter[hj(ai)] = 1
        end foreach
  end foreach
  return filter
```

VI. CONCLUSION

We addressed the problem of securely transmitting data for sensor networks, and proposed a data encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of data. We extended the scheme to incorporate data binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, we plan to implement a real system prototype of our secure scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

[1] Yunus Sarikaya, C. Emre Koksal, Senior Member, IEEE, and Ozgur rcetin,"Dynamic Network Control for Confidential Multi-Hop Communications", IEEE/ACM Transactions on Networking, vol. 24, no. 2, APRIL 2016.
[2] Nof Abuzainab, Student Member, IEEE, and Anthony Ephremides, Life Fellow, IEEE, "Secure Distributed Information Exchange", IEEE Transactions on Information Theory, vol. 60, no. 2, February 2014.
[3] Tao Cui, Student Member, IEEE, TraceyHo, Senior Member, IEEE, and Jörg Kliewer, Senior Member, IEEE," On Secure Network Coding With Nonuniform or Restricted Wiretap Sets", IEEE Transactions on Information Theory, vol. 59, no. 1, January 2013.
[4] Hamza Aldabbas, Tariq Alwada'n, Helge Janicke, Ali Al-Bayatti," Data Confidentiality in Mobile Ad hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 1, February 2012.
[5] C. Emre Koksal, Ozgur Ercetin, Yunus Sarikaya," Control of Wireless Networks with Secrecy, [cs.IT] 25 Apr 2012.
[6] Lun Dong, Member, IEEE, Zhu Han, Senior Member, IEEE, Athina P. Petropulu, Fellow, IEEE, and H. Vincent Poor, Fellow, IEEE," Improving Wireless Physical Layer Security via Cooperating Relays", IEEE Transactions on Signal Processing, vol. 58, no. 3, March 2010.
[7] Ashish Khisti, Member, IEEE, and Gregory W. Wornell, Fellow, IEEE," Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel", IEEE Transactions on Information Theory, vol. 56, no. 7, July 2010.
[8] Onur Gungor, Jian Tan, Can Emre Koksal, Hesham El Gamal, Ness B. Shroff," Joint Power and Secret Key Queue Management for Delay Limited Secure Communication", IEEE INFOCOM 2010.