Secure Distributed Information Exchange in WSN

Aarati S. Gaikawad[1], Apurva Sali[2], Bhagyashri Kolhe[3], Shrija Verma[4], Shubhashri Raut[5]
[1, 2, 3, 4, 5] Department of Information Technology
[1, 2, 3, 4, 5]Dr. D. Y. Patil College of Engineering, Akurdi

Abstract*-Large-scale sensor 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 multihop networks in which multiple source-destination pairs communicate confidential messages, to be kept confidential from the intermediate nodes. We pose the problem as that of network utility 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.*

We propose a novel lightweight scheme to securely transmit data for sensor 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 functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate 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.

I. INTRODUCTION

In some scenarios (e.g.,tactical, financial, medical), confidentiality of communicated information between the nodes is necessary, so that data intended to(or originated from) a node is not shared by any other node. 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 uncaptured nodes. In this project, 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 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 project, we build efficient algorithms for confidential multiuser communication over multihop wireless networks without the source-destination pairs having to share any secret key a priori. The metric we use to measure the confidentiality is the mutual information leakage rate to the relay nodes, i.e., the equivocation rate. We require this rate to be arbitrarily small with high probability and impose this in the resource allocation problem via an additional constraint.

The problem of network control with confidential messages has been studied in the past for the single-hop setting. 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. In addition, the existing schemes for wireless multihop networks are not concerned with how information ought to be spatially distributed in the network. Hence, unlike the standard multihop dynamic algorithm where the objective is to only increase end-to-end flow rates, in our problem, increasing the flow rate and keeping confidentiality of the messages appear as two conflicting objectives.

1.1 Why Network Security Is Important ?

Network Security is a branch of computer science that involves in securing a computer network and network infrastructure devices to prevent unauthorized access, data theft, network misuse, device and data modification. Network Security prevents DoS (Denial of Service) attacks and assures continuous service for legitimate network users. Network Security involves proactive defence methods and mechanisms to protect data, network and network devices from external and internal threats.

Data is the most precious factor of today's businesses. Top business organizations spend billions of dollers every year to secure their computer networks and to keep their business data safe. We are dependent on computers today for controlling large money transfers between banks, insurance, markets, telecommunication, electrical power distribution, health and medical fields, nuclear power plants, space research and satellites. We cannot negotiate security in these critical areas.

As the internet evolves and computer networks become bigger and bigger, network security has become one of the most important factors for companies to consider. Big enterprises like Microsoft are designing and building software products that need to be protected against foreign attacks. By increasing network security, you decrease the chance of privacy spoofing, identity or information theft and so on.

Piracy is a big concern to enterprises that are victims of its effects. Anything from software, music and movies to books, games, etc. are stolen and copied because security is breached by malicious individuals. Because hacker tools have become more and more sophisticated, super-intelligence is no longer a requirement to hack someone's computer or server. Of course, there are individuals that have developed sophisticated skills and know how to breach into a user's privacy in several ways, but these types of individuals are less common than in the past. Today, most malicious users do not possess a high level of programming skills and instead make use of tools available on the Internet. There are several stages that an attacker has to pass through to successfully carry out an attack.

1.2 How Do Security Breaches Happen ?

If someone can gain enough information and holds the necessary computing skills, he/she can compromise a company's network security somewhat easily. Because network security is mitigated by humans, it is also often susceptible to human mistakes. Anything from misconfigured equipment or services to unsecured usernames and passwords can pose a real threat to network security. Some default security holes of Operating Systems, network devices or TCP/IP protocols can be used by hackers to gain access to network resources.

There are known attacks in which protocol's weaknesses are exploited by attackers. Some of these protocols include SNMP, SMTP, HTTP, FTP or ICMP. It is important to update device's firmware, install the latest OS security updates and change the default settings. Every company should implement a security policy where potential vulnerabilities are addressed and treated.

Network attacks are often caused by direct or indirect interaction of humans. There are many situations in which employees themselves pose the biggest threat to enterprises. Many times, employees will unintentionally install piracy software that is infected with viruses, worms or trojans. Other times, users may forget to secure their workstations, leaving them open as an easy target to potential attackers. And yet others may give sensitive information to outsiders, or even play a role in an important part of an attack. (Power Admin's PA File Sight can help identify when sensitive or secure files have been accessed, deleted or copied to other drives.)

This is why a security policy should include internal and external threats. By gaining physical access to network devices, a user can extract important information from the company's servers or storage devices. Such attacks depend on the hacker's skills because without the proper tools, the success percentage is low. External attackers gain access to network resources through the internet, which is a very common way network security is compromised. We can group network attacks by the skills possessed by the attacker. Based on these criteria we can divide attacks in two categories:

i. **Unstructured** – attacks made by unskilled hackers. Individuals behind these attacks use hacking tools available on the Internet and are often not aware of the environment they are attacking. These threats should not be neglected because they can expose precious information to malicious users.

ii. **Structured** – attacks made by individuals who possess advanced computing skills. Such hackers are experts in exploiting system vulnerabilities. By gaining enough information about a company's network, these individuals can create custom hacking tools to breach network security. Most structured attacks are done by individuals with good programming skills and a good understanding of operating systems, networking and so on.

In today's data networks there are many different types of attacks and each one requires special skills that hackers must poses in order to successfully crack into someone's privacy:

1.3.1 Eavesdropping:- It is one of the common types of attacks. A malicious user can gain critical information from "listening" to network traffic. Because most communications are sent unencrypted, there are many cases in which traffic is susceptible to interception. The traffic can be analyzed using sniffing tools (also known as snooping) to read information as it is sent into the network. Wireless networks are more susceptible to interception than wired ones. Eavesdropping can be prevented by using encryption algorithms.

Dos and DDoS attacks (Denial of Service and Distributed Denial of Service attacks) – These attacks take advantage of network traffic to create abnormal behavior to network services or applications. Servers are often targeted and flooded with data until they become unreachable. Core network equipment can be blocked and thus prevent normal traffic from flowing into the network. Distributed denial of service attacks are more dangerous because attacks are made from multiple sources.

1.3.2 Password attacks :- These attacks are based on cracking user or equipment passwords. They are one of the most feared network attacks because once a user is compromised, the whole network can be damaged, especially if we are talking about a domain user or network administrator.

1.3.3 Dictionary attacks :- These use patterns to guess passwords in multiple attempts. Critical information can be gained by using a compromised username. This is one of the main reasons companies use strong passwords that are changed frequently.

1.3.4 Compromised-Key attack:- By obtaining the private key of a sender, an attacker can decipher secured network traffic. This kind of attack is often hard to be carried out successfully because it requires good computing resources and skills.

1.3.5 Man-in-the-Middle attack :– As the name implies, this attack is based on intercepting and modifying information between two transmitting nodes. A hacker can modify network routes to redirect traffic to its machine before it is carried out to the destination.

1.3.6 IP address spoofing :– in this scenario hackers use spoofed IPs to impersonate a legitimate machine. The attacker can then modify packets making them look like legitimate traffic to the receiving network device.

1.3.7 Computer Virus and Trojans Application-layer attacks :– these attacks are based on cracking applications that run on servers or workstations. These types of attacks are common because there are many different applications that run on machines and are susceptible to attacks. Hackers use viruses, Trojans and worms to infect devices and gain important information.

1.3.8 Exploit attacks :– These are usually made by individuals who possess strong computing skills and can take advantage of software bugs or misconfigurations. By having enough information of a specific software, hackers can “exploit” a particular problem and use it to gain access to private data.

II. RELATED WORK

In 2006, Wojciech Galuba and Panos Papadimitratos in their paper named “Castor: Scalable Secure Routing for Ad Hoc Networks” proposed a novel design design that made Castor resilient to a wide range of attacks and allowed the protocol to scale to large network sizes and remained efficient under high mobility. Their protocol achieved up to two times higher packet delivery rates, particularly in large and highly volatile networks, while incurring no or only limited additional overhead. At the same time, Castor was able to survive more severe attacks and recovered from them faster.

In 2007, Giuseppe Ateniese and Randal Burns in their paper named “Provable Data Possession at Untrusted Stores” introduced a modelfor provable data possession (PDP) that allowed a client that had stored data at an untrusted server to verify that the server possessed the original data without retrieving it. The model generated probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintained a constant amount of metadata to verify the proof. The challenge/response protocol transmitted a small, constant amount of data, which minimized network communication.

In 2008,Baruch Awerbuch ,Reza Curtmola David Holmer in their paper named “An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks” proposed ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provided resilience to Byzantine attacks caused by individual or colluding nodes. The protocol used an adaptive probing technique that detected a malicious link after log n faults have occurred, where n is the length of the path. Problematic links were avoided by using a route discovery mechanism that relied on a new metric that captured adversarial behavior.

In 2009 William Kozma Jr. and Loukas Lazos in their paper named “Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits” investigated the problem of uniquely identifying the set of misbehaving nodes which refused to forward packets. They proposed a novel misbehavior identification scheme called REAct that provided resource-efficient account ability for node misbehavior. REAct identified misbehaving nodes based on a series of random audits triggered upon a performance drop.

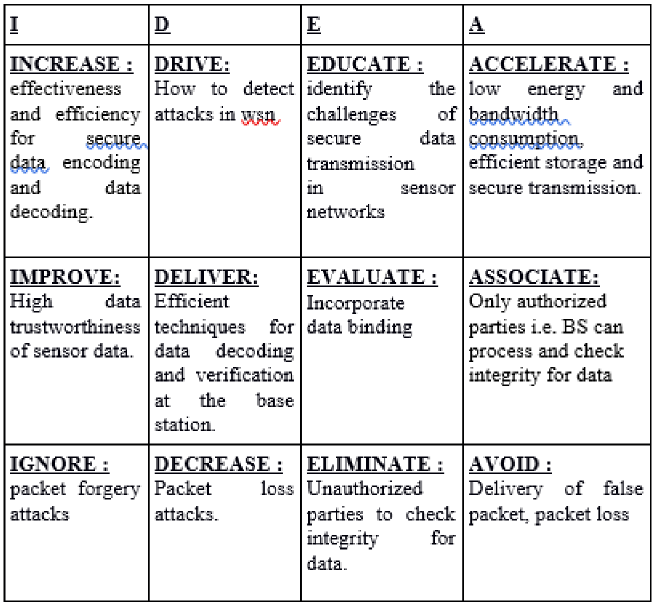
In 2010, Tao Shu, Sisi Liu, and Marwan Krunz in their paper named “Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes” proposed development mechanisms that generated randomized multipath routes. Under their design, the routes taken by the “shares”of different packets changed over time. So even if the routingalgorithm became known to the adversary, the adversary stillcannot pinpoint the routes traversed by each packet. Besidesrandomness, the routes generated by their mechanisms were alsohighly dispersive and energy-efficient, making them quite capableof bypassing black holes at low energy cost. Extensive simulationswere conducted to verify the validity of their mechanisms.

In 2014 Cong Wang, Qian Wang, and Kui Ren Wenjing Lou in their paper named “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing” uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which met all above requirements. To support efficient handling of multiple auditing tasks, they further explored the technique of bilinear aggregate signature to extend the main result into a multi-user setting, where TPA could perform multiple auditing tasks simultaneously. Extensive security and performance analysis showed the proposed schemes were provably secure and highly efficient

III. PROPOSED WORK

We investigate the problem of secure and efficient data transmission and processing for sensor networks, and we use data to detect packet loss attacks staged by malicious sensor nodes. Our goal is to design a efficient encoding and decoding mechanism that satisfies such security and performance needs. We propose a encoding strategy whereby each node on the path of a data packet securely embeds information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the data information. We also devise an extension of the data encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node. We use only fast message authentication code (MAC) schemes and Bloom filters, which are fixed-size data structures that compactly represent data. Bloom filters make efficient usage of bandwidth, and they yield low error rates in practice. We formulate the problem of secure data transmission in sensor networks, and identify the challenges specific to this context. We perform a detailed security analysis and performance evaluation of the proposed data encoding scheme and packet loss detection mechanism.The idea matrix is as follows

Idea Matrix



I	D	E	A
INCREASE : effectiveness and efficiency for secure data encoding and data decoding.	DRIVE: How to detect attacks in wsn	EDUCATE : identify the challenges of secure data transmission in sensor networks	ACCELERATE : low energy and bandwidth consumption. efficient storage and secure transmission.
IMPROVE: High data trustworthiness of sensor data.	DELIVER: Efficient techniques for data decoding and verification at the base station.	EVALUATE : Incorporate data binding	ASSOCIATE: Only authorized parties i.e. BS can process and check integrity for data
IGNORE : packet forgery attacks	DECREASE : Packet loss attacks.	ELIMINATE : Unauthorized parties to check integrity for data.	AVOID : Delivery of false packet, packet loss

We have made an idea matrix in oreder to implement transmission of confidential messages in distributed system in Wireless Sensor Networks.

Our objective is to develop a stationary control policy giving joint scheduling and routing decisions that achieves end-to-end confidential transmission of information. We state a network utility maximization problem and provide a scheme that maximizes aggregate network utility while achieving perfect secrecy over infinitely many blocks. We develop our solution based on the following assumptions:

A1. We consider the large block size asymptotics, i.e., secrecy encoding is across blocks.
A2. There is a centralized scheduler with the perfect knowledge of instantaneous CSI of all channels.
A3.The secrecy encoding rate is fixed: source node uses the encoder.

Assumption A1. allows our developed mechanisms to react to an undesirably large rate of accumulation at a given node at a time scale faster than the number of blocks across which the message is encoded.

Assumption A2. can be achieved by nodes sending their CSI to the centralized scheduler at the expense of increased control overhead.

Assumption A3. states that the a priori encoding rate of the message may not maximize the confidential throughput of the source node. Next, we develop a dynamic algorithm taking as input the queue lengths and the accumulated information at the intermediate nodes, and gives as output the scheduled node and the admitted confidential flows into the queues of the sources.

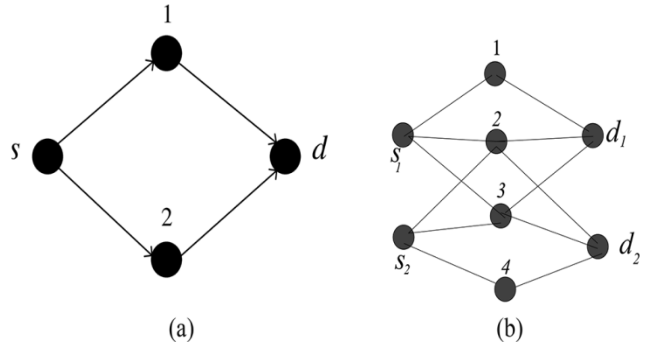


Fig. 1. Network models. (a) Diamond network. (b) Multi-network.

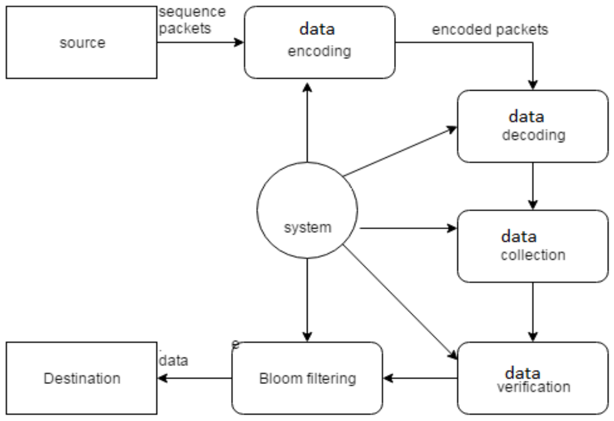


Fig. 2. Data flow diagram using bloom filter algorithm

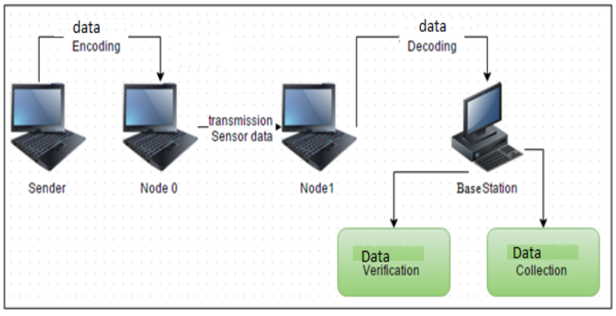


Fig. 3. System Architecture

IV.MATHEMATICAL MODEL

Let S be the Whole system which consists:
S= {IP, Pro, OP}.
Where,
A.IP is the input of the system.
B.Pro is the procedure applied to the system to process the given input.
C.OP is the output of the system.

A. Input:

IP = {U, F, dp, sn}.
Where,

1.U be the user.
U = {u1, u2, u3 … .. . un}.
2.F be set of files used for sending.
F = {f1, f2, f3 . . . . . fn}.
3.sn be sequence number assigned to each data packets.
4.Dp be data packets here, the system will divide data into 3 different packets.

B. Process

1. Source node sends data toward the destination node**.**
2. The system will divide the data which is sending the sender to destination node into 3 dp assigns the sn to each dp.
3. The middle pc or intermediate pc will be receiving the packets from sender and forwarding to next node and this process continues till data reaches to destination node.
4. at destination the packet drop attack will detected on the basis of sequence numbers. The system collects the both sequence number from sender as well as receiver and compares them if the system founds the difference in particular sequence number then receiver and sender both will be notified by alert message about packet drop attack this process is known as decoding.

C. Output:

Proper Detection of packet drop attack will be done at destination.

V. CONCLUSION

In this project, 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 over time-varying uplink channels, all intermediate nodes are considered as internal eavesdroppers from which the confidential information needs to be protected. To provide confidentiality in such setting, we proposed encoding the message over long blocks of information which are transmitted over different paths.

We have designed a dynamic control algorithm for a given encoding rate and we proved that our algorithm achieves utility arbitrarily close to the maximum achievable utility. In this problem, we have found out that increasing the flow rate and keeping confidentiality is two conflicting objective unlike standard dynamic algorithms, and the algorithm also considers spatial distribution of the flows over each path. We considerd the system, where the messages are encoded over finite number of blocks. For this system, transmissions of each block of the same message are dependent with each other. Thus, sub-optimal algorithm is applied and the considered algorithm approaches the optimal solution as the number of blocks which the message are encoded, increases.

We have dealt with implementation issues of the algorithms. First, we decreased overhead imposed by the updates transmitted to the scheduler. For that purpose, we design infrequent queue update algorithm, where users updated their queue length information periodically. We showed that this algorithm again approaches the optimal solution in the expense of increasing average queue lengths. Then, we investigated distributed version of our dynamic control algorithms, where the scheduler decision is given according to local information available to each node. We have proposed the use of the results of hashing data packets as session keys to encrypt these same data packets. The re-keying process between one sender and multiple receivers can be done in this way on the reception of the data packets without requiring any additional energy expensive mechanisms.

REFERENCES

[1] L. Georgiadis, M.J. Neely, and L. Tassiulas, "Resoruce allocation and cross-layer control in wireless networks," Found. Trends Netw., vol. 1, no. 1, pp. 1–144, 2006. SARIKAYA etal : DYNAMIC NETWORK CONTROL FOR CONFIDENTIAL MULTI-HOP COMMUNICATIONS 1195.

[2] X. Lin, N. B. Shroff, and R. Srikant, " On the connection - level stability of congestion- controlled communication networks, " IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2317– 2338, May 2008.

[3] Y. Chen, R. Hwang, and Y. Lin, "Multipath qos routing with bandwidth guarantee," in Proc. 2001 IEEE Global Telecommun. Conf., San Antonio, TX, USA, Sep. 2001, vol. 4, pp. 2199–2203.

[4] X. Lin and N. B. Shroff, " Utility maximization for communication networks with Multipath routing," IEEE Trans. Autom. Contr., vol. 51, no. 5, pp. 766–781, May 2006.

[5] A. D. Wyner, "The wire - tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–138, Oct. 1975.

[6] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[7] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[8] O. Gungor, J. Tan, C. E. Koksal, H. E. Gamal, and N. B. Shroff, "Joint power and secret key queue management for delay limited secure communication," presented at the IEEE INFOCOM 2010, San Diego, CA, USA, Mar. 2010.

[9] A. Khisti and G. W. Wornel, "Secure transmissions with multiple antennas: The misome wiretap channel," IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3014, July 2010.

[10] S. Shaffiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of gaussian mimo wire- tap channel: The 2-2-1 channel," IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4033–4039,Sep. 2009.