ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A New Binary Key Network Coding Scheme to Reduce Transmission Cost and Detect Data Polluters in Networks

R. Reshma Sony[1], V.Vijayaganth[2,] M.Suganya[3]

ME Student, Dept. of Computer Science, CSI College of Engineering, Ketti, The Nilgiris, Tamil Nadu, India[1]

Asst. Professor, Dept. of Computer Science, CSI College of Engineering, Ketti, The Nilgiris, Tamil Nadu, India [2]

ME Student, Dept. of Computer Science, CSI College of Engineering, Ketti, The Nilgiris, Tamil Nadu, India[3]

ABSTRACT: Data security and data protection against data modification attacks with resource efficiency are the major challenging tasks of Networks. Packet dropping and modifications are also common attacks that can be launched by an adversary to disrupt communication in networks. Many schemes have been proposed to mitigate, prevent those attacks. But very few can efficiently identify the data modification attackers with the delay and cost considerations. Even those schemes could find after the attacks done. Those type of schemes used packet BinD-Key ing techniques to investigate and verify the security issue. And that type of implementation is not considered the communication and energy overhead. To address these issues, the proposed system introduces a simple and powerful scheme. The scheme which is a rapid identifier of polluters and this helps to identify misbehaved data and routes that dropped or modified packets. And this proposed system also considers the other type of security issues such as data modification attacks, packet content modification and packet dropping attacks. In order to identify and prevent the data from unauthorized forwarders, the system proposed a new scheme which is named as BinD-Key (**Binary Encode Decode**-Key). The proposed system utilizes the BinD-Key which is an efficient packet BinD-Keying technique to protect, prevent and avoid routing misbehaving attacks. In order to identify and block the nodes which tries to drop or modify the data, the proposed system has been implemented the key_bit verification algorithm. The proposed system also recovers the data which are polluted and retransmits using cache based recovery concept. The procedure behind the proposed system is to identify the key and its value of every packet with secured data transmission.

KEYWORDS: Key, Packet, hop, encoding, decoding, network coding, attacker

I. INTRODUCTION

Network coding is coding at a node in a packet network (where data is divided into packets and network coding is applied to the contents of packets), or more generally, coding above the physical layer. On the other network information theory is generally concerned with coding at the physical layer. This type of packet networks limits scope of unnecessarily, and some results with implications beyond packet networks may not be reported. A pollution attack defines injecting malicious packets in the network. The pollution attacks are amplified by the network coding process, resulting in a greater damage than under traditional routing.

Network coding allows intermediate nodes between the source(s) and the destinations not only to store and forward, but also to encode the received packets before forwarding them. The linear coding suffices to achieve the max-flow from the source to each receiving node in multicast networks, where intermediate nodes generate outgoing packets as linear combinations of their incoming packets. The proposed a network coding framework that allows to deal with random packet loss, change of topology, and delays. Network coding offers various advantages.

- Maximizing the usage of network resources
- Robustness to network impairments and
- Packet losses, even in dynamic networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

An honest intermediate node receiving a single malicious packet would perform the encoding of the malicious packet with other packets, resulting in multiple corrupted outgoing packets that are then forwarded on to the next nodes.

NEED OF WIRELESS NETWORK CODING:

Wireless networks have been designed using the wired network as the blueprint. The design abstracts the wireless channel as a point-to-point link, and grafts wired network protocols onto the wireless environments. For example, routing uses shortest path protocols, routers forward packets but do not modify the data, and reliability relies on retransmissions. The design has worked well for wired networks, but less so for the unreliable and unpredictable wireless medium. The wireless medium is fundamentally different. While wired networks have reliable and predictable links, wireless links have high bit error rate, and their characteristics could vary over short time-scales. Further, wired links are unicast links, but the majority of wireless links (with Omni-directional antennas) are broadcast links. Transmissions in a wired network do not interfere with each other, whereas interference is a common case for the wireless medium. Wired nodes are usually static, while wireless was built to support mobility and portability. The wired network design conflicts with the characteristics of the wireless medium. As a result, current wireless networks suffer low throughput, dead spots, and inadequate mobility support. The characteristics of wireless networks might all seem disadvantageous at first sight, but a newer perspective reveals that some of them can be used to our advantage, albeit with a fresh design. The broadcast nature of wireless provides an opportunity to deal with unreliability; when a node broadcasts a packet, it is likely that at least one nearby node receives it, which can then function as the next-hop and forward the packet. This is in stark contrast to the present wireless design, where there is a single designated next-hop, and when it does not receive the packet, the previous hop has to retransmit it.

II. LITERATURE SURVEY

In [1] Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects false data into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes. Standard authentication mechanisms cannot prevent this attack if the adversary has compromised one or a small number of sensor nodes. In this paper, we present an interleaved hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised.

Further, our scheme provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to t colluding compromised nodes. We show that in the worst case B is O (t2). We also propose a variant of this scheme which guarantees B = 0 and works for a small t. Through Performance analysis, we show that our scheme is efficient with respect to the security it provides, and it also allows a tradeoff between security and performance. In this paper, they presented a simple but effective authentication scheme to prevent false data injection attacks in sensor networks. The scheme guarantees that the base station can detect a false report when no more than t nodes are compromised, where t is a security threshold. In addition, our scheme guarantees that t colluding compromised sensors can deceive at most B non compromised nodes to forward our performance analysis shows this scheme is efficient with respect to the security it provides and allows a tradeoff between security and performance. [2] Numerous authentication schemes have been proposed in the past for protecting communication authenticity and integrity in wireless sensor networks. Most of them however have following limitations: high computation or communication overhead, no resilience to a large number of node compromises, delayed authentication, lack of scalability, etc. To address these issues, we propose in this paper a novel message authentication approach which adopts a perturbed polynomial-based technique to simultaneously accomplish the goals of lightweight, resilience to a large number of node compromises, immediate authentication, scalability, and non-repudiation. Extensive analysis and experiments have also been conducted to evaluate the scheme in terms of security properties and system overhead. They proposed a novel message authentication approach which adopts a perturbed polynomial-based technique to simultaneously accomplish the goals of lightweight, resilience to node compromises, immediate authentication, scalability, and non-repudiation.[3] Wireless sensor networks (WSNs) are increasingly used in many applications, such as volcano and fire monitoring, urban sensing, and perimeter surveillance. In a large WSN, in-network data aggregation (i.e., combining partial results at intermediate nodes during message routing) significantly reduces the amount of communication overhead and energy consumption. The research community proposed a loss-resilient aggregation framework called synopsis diffusion, which uses duplicate insensitive algorithms on top of multipath routing schemes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

to accurately compute aggregates (e.g., predicate count or sum). However, this aggregation framework does not address the problem of false subaggregate values contributed by compromised nodes. This attack may cause large errors in the aggregate computed at the base station, which is the root node in the aggregation hierarchy. In this paper, we make the synopsis diffusion approach secure against the above attack launched by compromised nodes. In particular, we present an algorithm to enable the base station to securely compute predicate count or sum even in the presence of such an attack. Our attack-resilient computation algorithm computes the true aggregate by filtering out the contributions of compromised nodes in the aggregation hierarchy. Extensive analysis and simulation study show that our algorithm outperforms other existing approaches. The system discussed the security issues of in-network aggregation algorithms to compute aggregates such as predicate Count and Sum. In particular, we showed the falsified sub-aggregate attack launched by a few compromised nodes can inject arbitrary amount of error in the base station's estimate of the aggregate. It presented an attack-resilient computation algorithm which would guarantee the successful computation of the aggregate even in the presence of the attack.[4] In a large-scale sensor network individual sensors are subject to security compromises. A compromised node can inject into the network large quantities of bogus sensing reports which, if undetected, would be forwarded to the data collection point (i.e. the sink). Such attacks by compromised sensors can cause not only false alarms but also the depletion of the finite amount of energy in a battery powered network. paper we present a Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. SEF requires that each sensing report be validated by multiple keyed message authentication codes (MACs), each generated by a node that detects the same event. As the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. SEF exploits the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes.

Sensor networks serving mission-critical applications are potential targets for malicious attacks. Although a number of recent research efforts have addressed security issues such as node authentication, data secrecy and integrity, they provide no protection against injected false sensing reports once any single node is compromised. SEF aims at detecting and dropping such false reports injected by compromised nodes. SEF's detection and filtering power increases with the deployment density and the sensor field size.

SEF can effectively detect false reports even when the attacker has obtained the security keys from a number of compromised nodes, as long as those keys belong to a small number of the key pool partitions. It can filter out 80∼90% false data by a compromised node within 10 forwarding hops. [5] Many application domains, such as real-time financial analysis, e-healthcare systems, sensor networks, are characterized by continuous data streaming from multiple sources and through intermediate processing by multiple aggregators. Keeping track of data provenance in such highly dynamic context is an important requirement, since data provenance is a key factor in assessing data trustworthiness which is crucial for many applications. Provenance management for streaming data requires addressing several challenges, including the assurance of high processing throughput, low bandwidth consumption, storage efficiency and secure transmission. propose a novel approach to securely transmit provenance for streaming data (focusing on sensor network) by embedding provenance into the inter packet timing domain while addressing the above mentioned issues. As provenance is hidden in another host-medium, our solution can be conceptualized as watemarking technique. However, unlike traditional watermarking approaches, we embed provenance over the inter packet delays (IPDs) rather than in the sensor data themselves, hence avoiding the problem of data degradation due to watermarking. Provenance is extracted by the data receiver utilizing an optimal threshold-based mechanism which minimizes the probability of provenance decoding errors. The resiliency of the scheme against outside and inside attackers is established through an extensive security analysis. Experiments show that our technique can recover provenance up to a certain level against perturbations to inter-packet timing characteristics.[6] The rapid advances in processor, memory, and radio technology have enabled the development of distributed networks of small, inexpensive nodes that are capable of sensing, computation, and wireless communication. Sensor networks of the future are envisioned to revolutionize the paradigm of collecting and processing information in diverse environments. However, the severe energy constraints and limited computing resources of the sensors, present major challenges for such a vision to become a reality. We consider a network of energy–constrained sensors that are deployed over a region. Each sensor periodically produces information as it monitors its vicinity. The basic operation in such a network is the systematic gathering and transmission of sensed data to a base station for further processing. During data gathering, sensors have the ability to perform in–network aggregation (fusion) of data packets enroute to the base station. The lifetime of such a sensor system is the time during

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

which we can gather information from all the sensors to the base station. A key challenge in data gathering is to maximize the system lifetime, given the energy constraints. Given the location of sensors and the base station and the available energy at each sensor, we are interested in finding an efficient manner in which the data should be collected from all the sensors and transmitted to the base station, such that the system lifetime is maximized. This is the maximum lifetime data gathering problem. We present an efficient clustering–based heuristic to solve the data gathering problem. Our experimental results demonstrate that the proposed algorithms significantly outperform previous methods, in terms of system lifetime. [7] The sharing of caches among Web proxies is an important technique to reduce Web track and alleviate net- work bottlenecks. Nevertheless it is not widely deployed due to the overhead of existing protocols. In this paper we propose a new protocol called \Summary Cache"; each proxy keeps a summary of the URLs of cached documents of each participating proxy and checks these summaries for potential hits before sending any queries. Two factors contribute to the low overhead: the summaries are updated only periodically, and the summary representations are economical { as low as 8 bits per entry. In particular, trace-driven simulations show that, compared to ICP, the new protocol reduces the number of inter-proxy protocol messages by a factor of 25 to 60, reduces the bandwidth consumption by over 50%, while incurring almost no degradation in the cache hit ratios. Simulation and analysis further demonstrate the scalability of the protocol. [8] A Bloom filter is a space-efficient data structure that answers set membership queries with some chance of a false positive. We introduce the problem of designing generalizations of Bloom filters designed to answer queries of the form, “Is x close to an element of S?” where closeness is measured under a suitable metric. Such a data structure would have several natural applications in networking and database applications.[9] Recent work on distributed, in-network aggregation assumes a benign population of participants. Unfortunately, modern distributed systems are plagued by malicious participants. In this paper we present a first step towards verifiable yet efficient distributed, in-network aggregation in adversarial settings. We describe a general framework and threat model for the problem and then present proof sketches, a compact verification mechanism that combines cryptographic signatures and Flajolet-Martin sketches to guarantee acceptable aggregation error bounds with high probability. We derive proof sketches for count aggregates and extend them for random sampling, which can be used to provide verifiable approximations for a broad class of data analysis queries, e.g., quantiles and heavy hitters. Finally, we evaluate the practical use of proof sketches, and observe that adversaries can often be reduced to much smaller violations in practice than our worst-case bounds suggest. Cryptographic authentication and approximate query processing is followed in this system. While this sounds complex, our FM-based proof sketches provide a remarkably simple defense against the introduction of spurious data during aggregation.

III. PROPOSED SYSTEM

Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders. To address this problem, this proposes a simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. The proposed system finds the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. This extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Encoding algorithm Steps:

The steps for encoding a tag value are specified below:

1. Initial tag value is assigned as decimal digits, initially it will be 0.
   Once it passed to another node then the tag will be updated.
2. Convert the decimal value to a binary value:
   For example: 0001
3. Break the binary value out into single-bit chunks (starting from the right hand side):
   101 01110
4. Convert each value to decimal:
   0011 → 3
5. If corruption occurred then add new bit with the decimal

   Ex: 30
6. If the data corrupted by another node then new bit will be added again.

   Ex: 301

The above algorithm is described about the steps followed in the key encoding process. The key is created using the security package of java (like java.Security). This encoding process is initialized with the zero number.Once the node start transmission then the key will be updated with the binary type. If node behaves improper then the key will be appended with the key (either 0 or 1). To verify the polluted node the key converted into decimal numbering and binary numbering is done frequently as in the above algorithm step 5.Because whenever the binary is converted as decimal. Then the appended bit can be identified easily. The key appended with the decimal number is more than one then there is more than one polluters are there.

Decoding Algorithm Steps:

The steps for decoding a tag value are specified below:

1. Get the code in the received data header packet.
2. Convert the decimal value to a binary value:
   For example: 0001
3. Break the binary value out into single-bit chunks (starting from the right hand side): 101 01110
4. Find the appended bit value in the code:
   00101
5. If corruption bit is found then verify with the each node tag on the header.
6. Identify the pollution node.
7. Intimate about the pollution node to monitor.

The reverse process of the encoding is done in the decoding process. The received tag is verified with the each node tag. If the appended bit is identified in any of the node tag then that node will be identified as polluter in the network. If it is identified while transmitting the data then the selected path is rejected to send the data other alternate path will be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

allotted to send the data to make data reliability in the communication. This is how the encoding and decoding algorithm is working.

IV. RESULTS AND DISCUSSION

Data Transmission Speed Comparison

The following chart shows the transmission speed comparison of proposed system with the existing system.

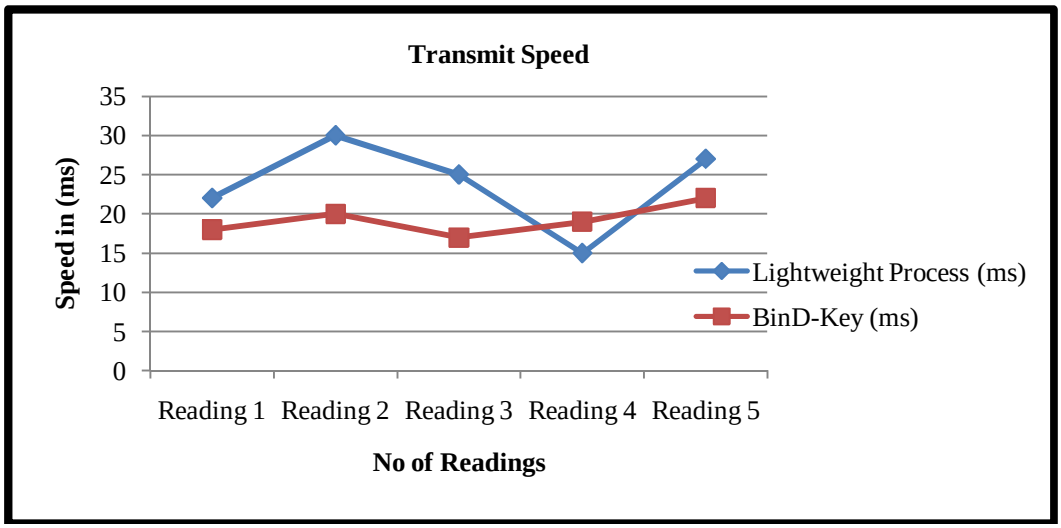

Fig 4.1 Transmission Speed Comparison Chart

Data Accuracy Comparison

Accuracy of the existing and proposed system are compared and deployed as follows.

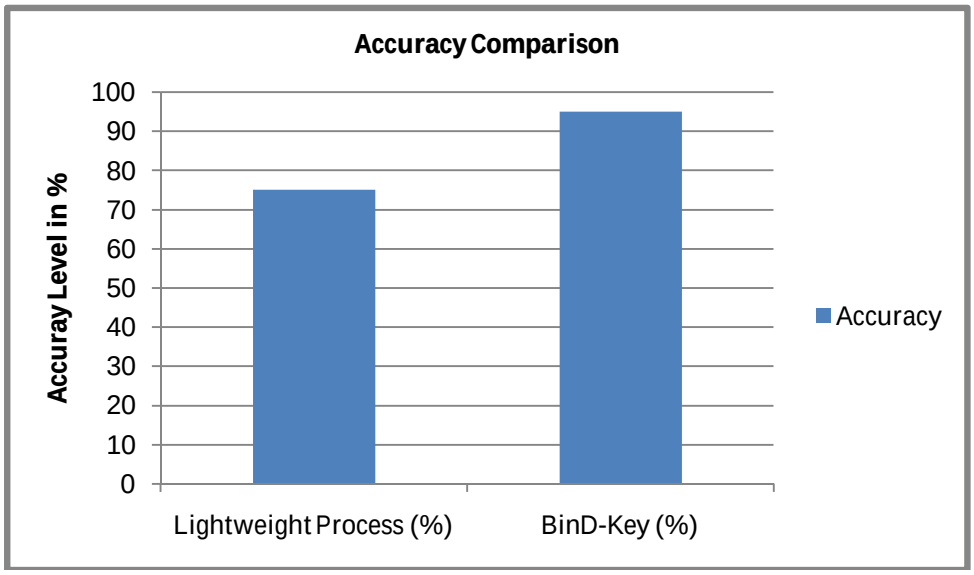

Fig 4.2 Accuracy Comparison Chart

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

V. CONCLUSION

This study addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. This extended the scheme to incorporate data-provenance 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 provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

[1] Zhu, Sencun, et al. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." *Security and privacy, 2004. Proceedings. 2004 IEEE symposium on*. IEEE, 2004
[2] Zhang, Wensheng, Nachiappan Subramanian, and Guiling Wang. "Lightweight and compromise-resilient message authentication in sensor networks."*INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008
[3] Roy, Sankardas, et al. "Secure data aggregation in wireless sensor networks."*Information Forensics and Security, IEEE Transactions on* 7.3 (2012): 1040-1052
[4] Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." *Selected Areas in Communications, IEEE Journal on* 23.4 (2005): 839-850
[5] Sultana, Shabana, Mohamed Shehab, and Elisa Bertino. "Secure provenance transmission for streaming data." *Knowledge and Data Engineering, IEEE Transactions on* 25.8 (2013): 1890-1903
[6] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in Sensor Networks," Proc. Wireless Comm. and Networking Conf., pp. 1948- 1953, 2003
[7] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000
[8] A.Kirsch and M. Mitzenmacher, "Distance-Sensitive BloomFilters," Proc.Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006
[9] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches: Verifiable In-Netwok Aggregation," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), pp. 84-89, 2007