International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

SINGLE BIT VERIFICATION MECHANISM TO IDENTIFY THE PACKET DROPPERS AND MODIFIERS

RajagopalT.K.P[1] ,Aravind G[2] ,Kanmani S[3],Mohammed Bagurudheen M[4]
[1]Associate professor,Computer Science And Engineering, Kathir College of Engineering,
[2,3,4] Computer Science And Engineering ,Kathir College of Engineering

Abstract- Data security and data protection against data modification attacks with resource ability are the major challenging tasks of Networks. Packet dropping and modifying are also common attacks that can be launched by an opponent to ruffle communication in networks. To address these issues, the proposed system introduces a simple and strong scheme. The scheme which is a effective identifier of polluters and this helps to identify bad-mannered data and routes that dropped or altered packets. And this suggested 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 illegal forwarders, the system proposed a new scheme which is named as MARK (Message Authentic Routing Key). The proposed system utilizes the MARK which is an efficient packet marking technique to protect, prevent and avoid routing bad-mannered attacks. In order to identify and block the nodes which tries to drop or modify the data, the proposed system has been enforced the key_bit verification algorithm. The proposed system also recovers the data which are spoiled and retransmit using cache based recovery concept. The procedure behind the proposed system is to identify the key and its value of every packets with secured data transmission.
Keywords: Finding packet droppers and modifiers, secured data transmission.

I. INTRODUCTION

Network coding is coding at a node in a packet network (where data is splited into packets and network coding is applied to the contents of packets), or more universally, 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 significance beyond packet networks may not be reported.

II. RELATED WORK

The splitting of caches among Web proxies is an important usage to uceuce Web track and alleviate net- work bottlenecks. Nevertheless it is not widely deployed due to the hanging of extant protocols. In this paper we propose a new protocol called “Summary Cache”; each proxy carry a brief of the URLs of cached documents of each participating proxy and checks these reviews for probable hits before sending any queries. Two factors contribute to the low overhead: the summaries are updated only periodically, and the brief representations are economical { as low as 8 bits per entry. In specific, trace-driven simulations show that, compared to ICP, the new protocol minimize the number of inter-proxy protocol messages by a factor of 25 to 60, reduces the bandwidth expenditure by over 50%, while incurring almost no degradation in the cache hit ratios. Proliferation and analysis further detemine the scalability of the protocol.

III. EXISTING SYSTEM

After mutual concession one or numerous nodes, an adversary may launch various attacks to disrupt the in-network communication. The attacks divided into two major problems, which are dropping packets and modifying Packets. Packets should not be filtered out while moving because

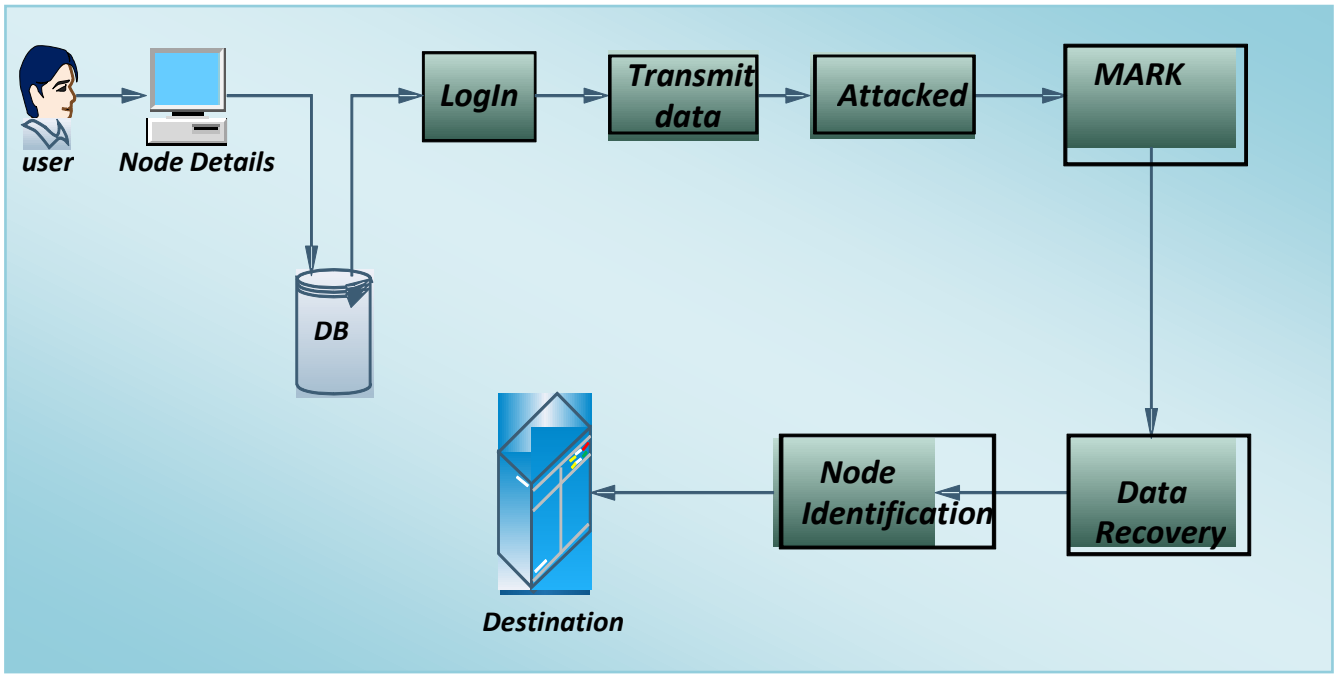
they should be used as clue to infer packet modifiers. So it cannot be used stable with existing packet filtering schemes this is a major problem of actual system.

To deal with packet droppers and polluters a widely support counter measure is used, which is multipath forwarding in that each packet is forwarded along several redundant paths and hence packet eliminating in some but not all of these paths can be tolerated.

Inherent weakness of network coding is that it is especially vulnerable to data modification attacks. Malicious nodes can inject corrupted packets into a network, which get mingled and forwarded by downstream nodes, thus causing a large number of damaged packets propagating in the network.

IV. PROPOSED SYSTEM

Packet dropping and modification are well known attacks that can be launched by an adversary to interrupt communication in wireless sensor networks. Many methods have been introduced to mitigate or tolerate such attacks, but very few can dramatically and efficiently identify the gate-crasher. To address this problem, this proposes a simple yet effective scheme, which can identify misconduct forwarders that drop or modify packets. The proposed system finds the problem of securely sending origin for sensor networks, and proposed a light-weight provenance encoding and decoding outline based on Bloom filters. The outline ensures security, integrity and freshness of provenance. This extended the scheme to incorporate data-provenance binding, and join packet sequence information that supports detection of packet loss attacks.



Methodologies:

MARK Mechanism Algorithm:

1. Encoding algorithm:
   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.

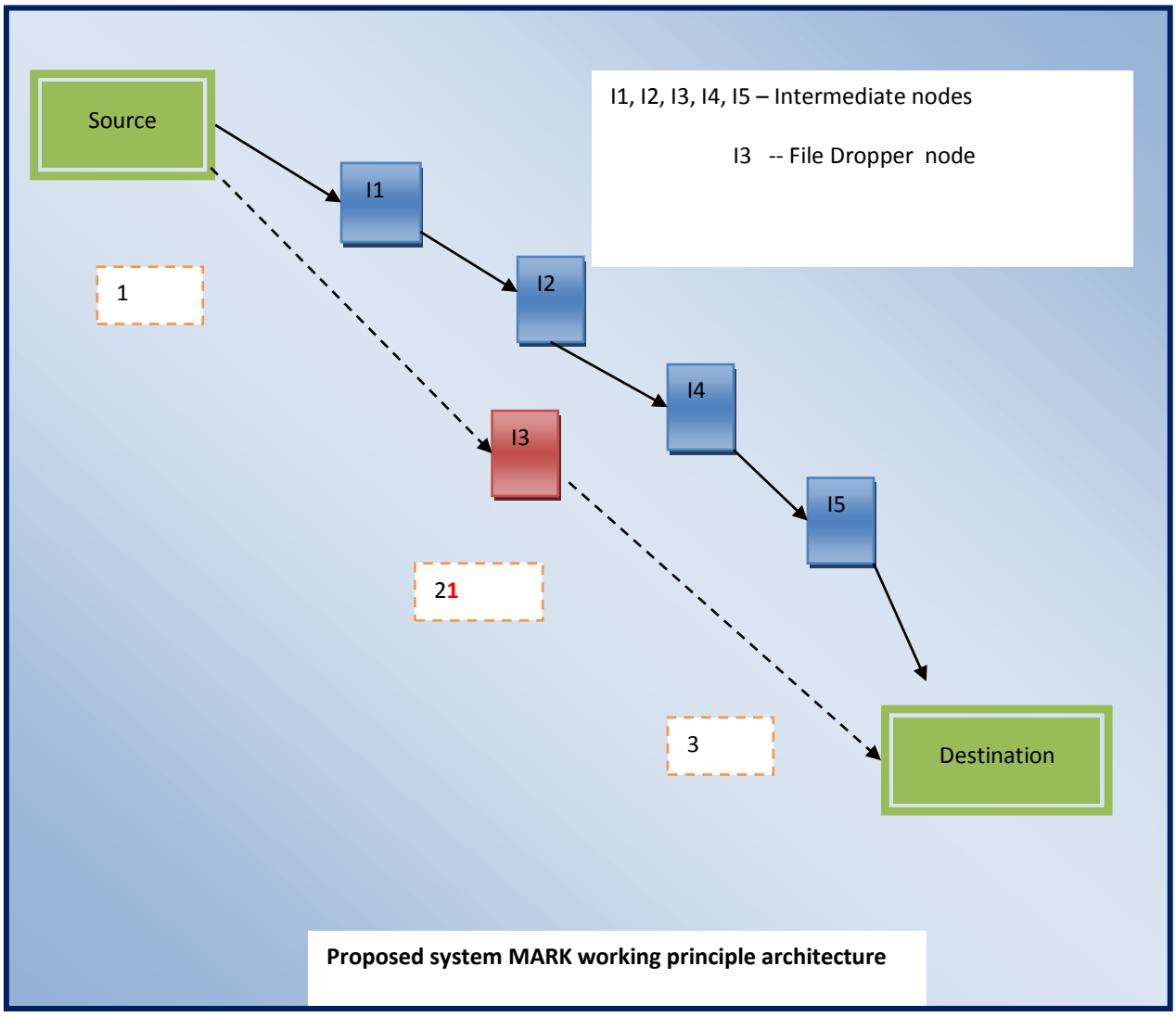
Ex: 301

2. Decoding Algorithm:

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.

MARK Algorithm Working Principle Diagram



V. CONCLUSION

In this proposed system in order to identify and prevent the data from unauthorized forwarders, the system expacted a new outline which is named as **MARK (Message Authentic Routing Key)**. The proposed system utilizes the MARK which is an efficient packet marking technique to protect, prevent and avoid routing misbehaving attacks. In order to identify and block the nodes which fling to drop or modify the data, the proposed system has been implemented the key_bit verification process. The proposed system also retrieve the data which are polluted and retransmits using cache based reconstruction concept

REFERENCES

1. Salmin Sultana, Gabriel Ghinita, Member, IEEE , Elisa Bertino, Fellow, IEEE , and Mohamed Shehab, Member, IEEE Computer Society
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. 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.

