INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 842-846
RECEIVED : 27/03/2016. PUBLISHED : 05/04/2016
April 5, 2016

VANDER: EFFICIENT COOPERATIVE WATCHDOG MONITORING FOR LOSSY WIRELESS NETWORK CODING

[1]S.Jayashree, [2]M.Kanimozhi, [3]V.Shobana, [4]K.Saravanan
[1,2,3,]Dept of Computer Science and Engineering, Pavai College Of Technology, Namakkal,
[4]HOD, Dept of Computer Science and Engineering, Pavai College Of Technology, Namakkal.

Abstract:

Network coding achieves the multicast network capacity throughput by allowing intermediate nodes to mix information in packets. The mixing operation network coding is vulnerable to pollution attacks. The newness of the proposed work is that when lossy overhearing happens: 1) watchdogs can cooperate with each other to share the packet information, where no extra overhead is introduced to normal transmission nodes; 2) rather than retransmitting all the lost packets among watchdogs, watchdogs use randomly generated Vandermonde hashes to detect the corrupted packet. VANDER can also detect successive colluded adversaries. Besides the provably low false alarm and misdetection probabilities, VANDER achieves low computational complexity and communication overhead. Numerical experiments are provided to support the theoretical analysis of VANDER. To identify application DOS attack, we propose a novel group testing (GT)-based approach deployed on back-end servers, which not only offers a theoretical method to obtain short detection delay and low false positive/negative rate, but also provides an Underlying framework against general network attacks. More specifically, we first extend classic GT model with size constraints for practice purposes, then redistribute the client service requests to multiple virtual servers embedded within each back-end server machine, according to specific testing matrices. Based on this framework, we propose a two-mode detection mechanism using some dynamic thresholds to efficiently identify the attackers. The focus of this work lies in the detection algorithms proposed and the corresponding theoretical complexity analysis. We also provide preliminary simulation results regarding the efficiency and practicability of this new Scheme. **Keywords:** VANDER, DOS

1. Introduction

Wireless Sensor Network

A wireless sensor network (WSN**)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, enabling also to control the activity of the sensors. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

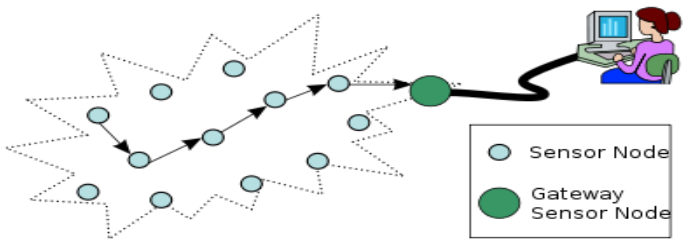


Fig 1.1typical multi-hop wireless sensor network architecture

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes"(demo video) of genuine microscopic dimensions have yet to be created.

Lossy Wireless Network

Network coding is a promising approach to achieve the maximum throughput of multicast networks. Since network coding requires that transitional network nodes mix received packet contents before forwarding, a single corrupted packet from the adversarial node can potentially contaminate all the information reaching the destination. Previous work on greenhouse gasses attacks in network coding transmissions can be categorized into three classes: information-theoretic, cryptographic, and watchdog-based approaches. The information-theoretic approaches and use end-to-end error correction codes to decode source messages. Thus, it makes minimal changes to existing network coding schemes; only the source and the sink are implicated in performing sophisticated computation to detect and correct errors introduced by malicious nodes. However, these schemes are geared toward a worst-case view of the adversarial action in which adversaries locate themselves at the weakest part of the network (the bottlenecks). In cryptographic solutions cryptographic primitives are used to enable honest network nodes to detect and drop corrupted packets. However, these approaches usually have high functioning complexity. In they conducted detailed analysis and experimental evaluation in realistic wireless network coding settings of the representative cryptographic methods.

2. Related Work

The seminal work first proved that multicast capacity (i.e., optimal throughput) can be achieved by introducing coding to the network nodes. The work and showed that linear network coding suffices to attain the capacity. Additionally rather than using global network topology in sequence to assemble network codes, low-complexity unsystematic linear network coding (RLNC) could achieve the competence in a circulated manner. As pollution attacks can make network coding quite inefficient or it can even damage transmissions in the whole network in the worst case researchers have proposed many methods to defend it. Existing work in protecting against pollution attacks in network coding falls into three categories: information-theoretic, cryptographic, and watchdog based schemes.

Information-Theoretic Schemes: In the information-theoretic approach, defences are handled in an end-to-end manner. Therefore, one can influence on error correction schemes while letting the intermediate nodes to put into practice standard network coding operations. In proposed a method in which receivers can detect defect attacks. The first polynomial-time network coding schemes that tightly achieve the error correction rate bounds. Recently efficient network coding manufacture has been proposed to attain the optimal error correction rates in the multiple-source scenarios. Cryptographic Schemes: homomorphism hash functions were used to verify the integrity of the packet. A secure channel to transmit hash values and the homomorphic signature scheme involves high computational complexity. Combined hash functions and RSA signatures to detect pollution attacks. It has proved that this scheme did not satisfy the required homomorphic property.

The proposed a non homomorphic signature scheme that used subspace checking to verify the packet. However, their scheme requires the source to know the whole file before the transmission. The scheme support data streaming by involving public key signatures for each individual vector. Compared with digital signature schemes, message authentication codes are used against pollution attacks. The

contaminated packet may not be identified at the first-hop downstream node; thus, it may pollute other packets.
To be precise, a third-party trusted node, watchdog overhears packet transmissions and detects pollution attacks. If the watchdog overhears all the receiving packets and the sending packets of a network node, any malicious behaviour of the network node can be efficiently detected by the watchdog. However, if a watchdog misses receiving packets of the monitored node (we term them upstream packets in the following) a justifiable packet would be falsely accused by this watchdog. Moreover, if a watchdog loses sending packets of the monitored node. This watchdog may miss detect the corrupted packet, which then pollutes the whole network transmissions. Previous work combined the idea of MDS (maximum-distance separable) codes to deal with watchdog lossy overhearing in multi hop routing networks.

3. Proposed Method:

To identify application DOS attack, we propose a novel group testing (GT)-based approach deployed on back-end servers, which not only offers a theoretical method to obtain short detection delay and low false positive/negative rate, but also provides an Underlying framework against general network attacks. More specifically, we first extend classic GT model with size constraints for practice purposes, then redistribute the client service requests to multiple virtual servers embedded within each back-end server machine, according to specific testing matrices.
Based on this framework, we propose a two-mode detection mechanism using some dynamic thresholds to efficiently identify the attackers. The focus of this work lies in the detection algorithms proposed and the corresponding theoretical complexity analysis. We also provide preliminary simulation results regarding the efficiency and practicability of this new Scheme.

4. Implementation

- Login Process Denial of Services.
- Group attacker modules.
- Group testing modules.
- Victim/Detection modules.

Login process denial of services

The login process by continually sending login-requests User enters an incorrect username and/or password, the application should respond with a generic error message stating that the information entered was incorrect. If the application explicitly states which component of the username/password pair was incorrect then an attacker can automate the process of trying common usernames from a dictionary file in an attempt to enumerate the users of the application.

Group attacker

Client provides a non spoofed ID, which is utilized to identify the client during our detection period. Despite that the application DoS attack is difficult to be traced; by identifying the IDs of attackers the firewall can block the subsequent malicious requests. The attackers are assumed to launch application service requests either at high inter arrival rate or high workload or even both. The term “request” refers to either main request or embedded request for HTTP page. Since the detection scheme proposed will be

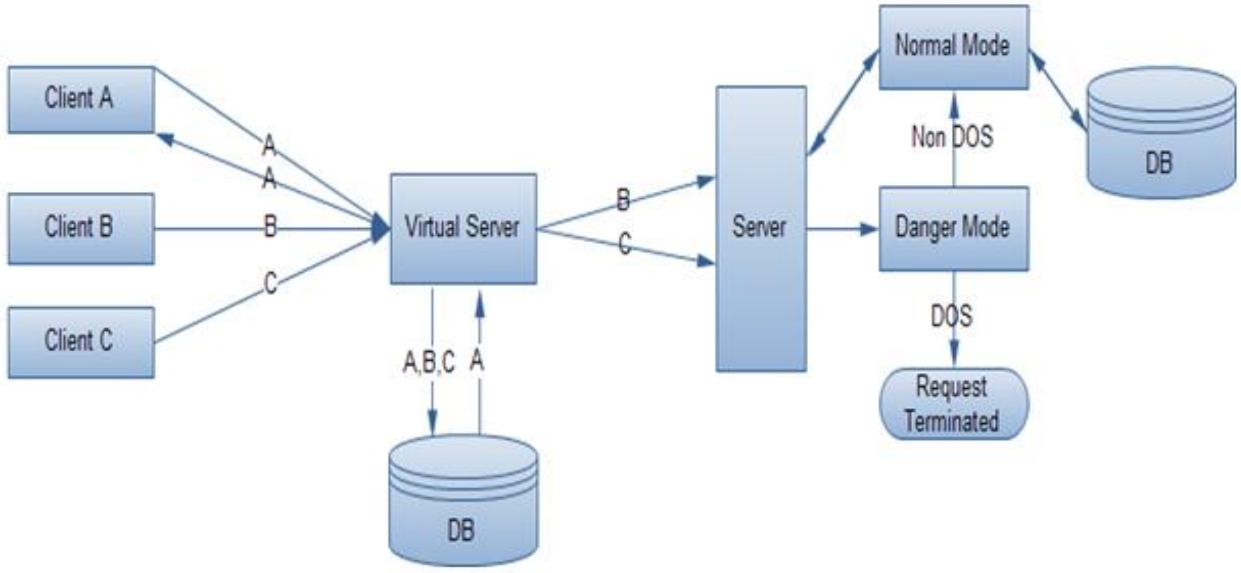
orthogonal to the session affinity, It do not consider the repeated one-shot attack mentioned in. We further assume that the number of attackers d << n where n is the total client amount.

Group testing

A positive outcome indicates that at least one positive item exists within this pool; whereas negative one means that all the items in the current pool are negative. A detection model based on GT can be assume that there are t virtual servers and n clients, among which d clients are . Binary testing matrix M and testing outcome vector V. Attackers

Victim/Detection modules

The victim model in our general framework consists of multiple back-end servers. Which can be Web/application servers, database servers, and distributed file systems? It do not take classic multitier Web servers as the model, since our detection scheme is deployed directly on the victim tier and identifies the attacks targeting at the same victim tier All the back-end servers provide multiple types of application services to clients using HTTP/1.1 protocol on TCP connections.



5. Conclusion

In this project investigated pollution attacks of lossy network coding in heterogeneous wireless networks. In meticulous helper nodes in heterogeneous wireless networks played the role of watchdogs that can overhear and monitor packet transmissions from the same wireless node. We proposed a novel watchdog cooperative monitoring scheme, i.e. VANDER, to address pollution attacks in the lossy wireless environment. In VANDER low overhead packets that contained random Vandermonde hashes were introduced to share packet information and check the validity of packets when lossy overhearing happened at watchdogs. As each column subspace of a Vandermonde matrix could be calculated efficiently only a small overhead was introduced among watchdogs, and no extra overhead was introduced to normal transmission nodes due to the cooperation.

References

1) R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1204–1216,Jul. 2000.
2) T. Hoet al., "Byzantine modification detection in multicast networks using randomized network coding," in Proc. IEEE ISIT, Jun./Jul. 2004,p. 143.
3) S. Jaggiet al., "Resilient network coding in the presence of Byzantine adversaries," IEEE Trans. Inform. Theory, vol. 54, no. 6, pp. 2596–2603,Jun. 2008.
4) M. Krohn, M. Freedman, and D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution," in Proc. IEEE Symp. Security , May 2004, pp. 226–40
5) C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in Proc. IEEE INFOCOM, Apr. 2006, pp. 1–13.
6) D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," in Proc. Conf. Inf. Sci. Syst., Mar. 2006, pp. 857–863.
7) Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signature-based scheme for securing network coding against pollution attacks," in Proc.of IEEE INFOCOM, Apr. 2008, pp. 2083–2091.