www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Exploiting the irregularity radio verify location in manet scattered

A. Elavarasi, Dr.P.Ramya

Department of Computer Science and Engineering, Mahendra Engineering College

ABSTRACT

Traditional distance-based Location Verification System (LVS) is ineffective for some attacks in sparse MANETs, e.g. the Similar Distance-based Malicious (SDM) attack. In this letter, we propose to exploit radio irregularity to build a novel LVS. Our system detects attack based on the estimated difference of radio irregularity coefficients, and the claimed locations of the malicious node and an assistant node. To the best of our knowledge, our system is the first-of-its-kind that can detect SDM attack and pollution attack with only the RSSI information transmitted by a detecting node to the suspicious malicious node and an assistant node. Simulation results demonstrate that our proposed system can detect the attacks that cannot be detected by traditional distance-based methods.

This paper assesses the effects of high-power jamming attacks in SDM optical networks utilizing Multi-Core Fibers (MCFs), where the disruptive effect of the inserted jamming signals may spread among multiple cores due to increased Inter-Core CrossTalk (ICo-XT). We first assess the jamming-induced reduction of the signal reach for different bit rates and modulation formats. The obtained reach limitations are then used to derive the maximal traffic disruption at the network level. Results indicate that connections provisioned satisfying the normal operating conditions are highly vulnerable to these attacks, potentially leading to huge data losses at the network level.

INTRODUCTION

Space Division Multiplexing (SDM) has been identified as a promising solution to the capacity crunch driven by the fast growth of bandwidth-intensive services. SDM enables ultra-high capacity in optical networks by utilizing a number of spatial resources, which can refer to multiple cores inside the same cladding of Multi-Core Fibers (MCFs); multiple modes inside the same core of Few-Mode Fibers (FMFs); or parallel single-mode fibers in the same bundle. In weakly-coupled MCFs, which are in the focus of this work, each core within the fiber is used as a distinct communication channel, assuming sufficiently low interference between neighboring cores. Key parameters determining the maximum transmission reach of optical signals in MCF are Amplified Spontaneous Emission (ASE) noise and Inter-Core CrossTalk (ICo-XT).

As the critical infrastructure enabling a plethora of vital societal services, optical networks can be an enticing target of deliberate attacks aimed at service disruption. High power jamming attacks, in which an attacking signal is inserted into the network via, e.g., direct access to the fiber plant, monitoring ports, or by bending the fiber, can be harmful to optical networks deploying different technologies. In networks based on Wavelength Division Multiplexing (WDM), this attack affects co-propagating user signals by increasing the Inter-Channel CrossTalk (ICh-XT) among channels traversing the same fiber (core). In SDM-based networks, the damaging potential of jamming signals can not only affect signals inside the same core, but it can also propagate to signals in adjacent cores via increased ICo-XT.

The primary requirement for increasing the network robustness to attacks is to evaluate the harmful effects caused by attacks and to quantify the damage they can cause to the network. While the damage from jamming attacks and the ways of increasing the level of physical-layer security in optical networks have been investigated in the context of Single-Mode Fibers (SMFs), the harmful

Author for correspondence:
Department of Computer Science and Engineering, Mahendra Engineering College

effects of jamming attacks in MCF-based SDM networks have not been studied so far.

NETWORK SECURITY

In this modern era, organizations greatly rely on computer networks to share information throughout the organization in an efficient and productive manner. Organizational computer networks are now becoming large and ubiquitous. Assuming that each staff member has a dedicated workstation, a large scale company would have few thousands workstations and many server on the network.

It is likely that these workstations may not be centrally managed, nor would they have perimeter protection. They may have a variety of operating systems, hardware, software, and protocols, with different level of cyber awareness among users. Now imagine, these thousands of workstations on company network are directly connected to the Internet. This sort of unsecured network becomes a target for an attack which holds valuable information and displays vulnerabilities.

Vulnerabilities & Attacks

The common vulnerability that exists in both wired and wireless networks is an "unauthorized access" to a network. An attacker can connect his device to a network though unsecure hub/switch port. In this regard, wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection.

After accessing, an attacker can exploit this vulnerability to launch attacks such as:

- Sniffing the packet data to steal valuable information.
- Denial of service to legitimate users on a network by flooding the network medium with spurious packets.
- Spoofing physical identities (MAC) of legitimate hosts and then stealing data or further launching a 'man-in-the-middle' attack.

Goals of Network Security

As discussed in earlier sections, there exists large number of vulnerabilities in the network. Thus, during transmission, data is highly vulnerable to attacks. An attacker can target the communication channel, obtain the data, and read the same or re-insert a false message to achieve his nefarious aims.

Network security is not only concerned about the security of the computers at each end of the communication chain; however, it aims to ensure that the entire network is secure.

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network.

The primary goal of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as **CIA triangle**.

Confidentiality

The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.

Integrity

This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

Availability

The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

Achieving Network Security

Ensuring network security may appear to be very simple. The goals to be achieved seems to be straightforward. But in reality, the mechanisms used to achieve these goals are highly complex, and understanding them involves sound reasoning.

International Telecommunication Union (ITU), in its recommendation on security architecture X.800, has defined certain mechanisms to bring the standardization in methods to achieve network security. Some of these mechanisms are:

En-Cipherment

This mechanism provides data confidentiality services by transforming data into not-readable forms for the unauthorized persons. This

mechanism uses encryption-decryption algorithm with secret keys.

Digital signatures

This mechanism is the electronic equivalent of ordinary signatures in electronic data. It provides authenticity of the data.

Access control

This mechanism is used to provide access control services. These mechanisms may use the identification and authentication of an entity to determine and enforce the access rights of the entity.

Having developed and identified various security mechanisms for achieving network security, it is essential to decide Where to apply them; both physically (at what location) and logically (at what layer of an architecture such as TCP/IP).

EXISTING SYSTEM

To detect the falsified location of a malicious node, some location verification systems (LVSs) have been proposed. Verified the location by comparing the estimated location and the claimed location of some node. Proposed a LVS for one-dimensional wireless Ad hoc networks based on the probability mass function of hop-count and the recorded hop-count. Moreover, mobility grade threshold-based verification, maximum density threshold-based verification and map-based verification are also proposed and analyzed by researchers. However, most of the existing LVSs need exact ranging to detect malicious node. In sparse MANETs, a malicious node could claim a falsified location to its neighbors when the real inter-node distance between the malicious node and its neighbor is similar to the claimed falsified inter-node distance. This type of malicious node is referred as a Similar Distance based Malicious (SDM) node, and its attack is called SDM attack. Note that pollution attack is a special case of SDM attack. Traditional distance based LVS is ineffective on handling SDM attacks.

To detect SDM attacks, several LVSs have been proposed, such as the use of covert mobile base stations, the random movement of nodes, a different network, the angle of arrival (AOA) of radio signal, or fingerprinting. However, in emerging sparse MANETs such as UAV networks, nodes are not allowed to hide their locations due to security reasons. Moreover, the mobility of nodes is limited in some network, and thus random movement is not appropriate in such case. In addition, it is hard to obtain the location of other nodes from a different network. Besides, the hardware for estimating AOA increases the size and overhead of a node, and a fingerprint database for outdoor area is too complicated to be built. Therefore, it is necessary for the compromised node to verify the claimed location of its neighbors.

Need for new system

Optical Signal-to-Noise Ratio (OSNR) requirements, which largely depend on the ASE noise, tighten with the increasing complexity of modulation formats, where more complex and spectrally efficient modulation formats require higher OSNR to achieve acceptable Bit Error Rate (BER) values. The transmission reach limitation due to noise is also inversely proportional to the signal bit rate, i.e., signals with higher bit rates have a shorter reach.

Proposed system

The work in proposes a design strategy that enhances the conventional Dedicated Path Protection (DPP) with attack-awareness. The above-mentioned studies show that physical-layer security can be enhanced while using the same amount of optical resources as conventional, resource-saving approaches. However, these works consider a WDM optical network where the damaging effects of jamming signals stay confined in a single fiber core. In SDM networks, signal interference among adjacent cores cannot be neglected, particularly in the presence of high-power jamming signals.

The models can be simplified assuming the worst-case ICo-XT scenario (i.e., the core with the highest number of adjacent cores), as well as applied to find transmission reaches of different modulation formats in the presence of ICo-XT.

Proposed approach

Optical Signal-to-Noise Ratio (OSNR) requirements, which largely depend on the ASE noise, tighten with the increasing complexity of

modulation formats, where more complex and spectrally efficient modulation formats require higher OSNR to achieve acceptable Bit Error Rate (BER) values. The transmission reach limitation due to noise is also inversely proportional to the signal bit rate, i.e., signals with higher bit rates have a shorter reach.

METHODOLOGY

Objective

To exploit radio irregularity to build a novel LVS. Our system detects attack based on the estimated difference of radio irregularity coefficients, and the claimed locations of the malicious node and an assistant node.

Dedicated Path Protection

The work in proposes a design strategy that enhances the conventional Dedicated Path Protection (DPP) with attack-awareness. The above-mentioned studies show that physical-layer security can be enhanced while using the same amount of optical resources as conventional, resource-saving approaches. However, these works consider a WDM optical network where the damaging effects of jamming signals stay confined in a single fiber core. In SDM networks, signal interference among adjacent cores cannot be neglected, particularly in the presence of high-power jamming signals.

The models can be simplified assuming the worst-case ICo-XT scenario (i.e., the core with the highest number of adjacent cores), as well as applied to find transmission reaches of different modulation formats in the presence of ICo-XT.

SYSTEM DESIGN

Consider three nodes, *A*, *B*, and *M*, in a sparse MANET. *B* is assumed to be a normal node whose location is convinced due to certain regulation or verification result. *M* is a malicious node. *A* is a neighbor of *B* and *M*. The latter two can obtain the RSSI (Received Signal Strength Indicator) from node *A* [2]. We assume that all the nodes cannot hide their own locations, neither can they obtain the locations of other nodes from a different network. Besides, traditional AOA and fingerprint information are assumed not available in our system.

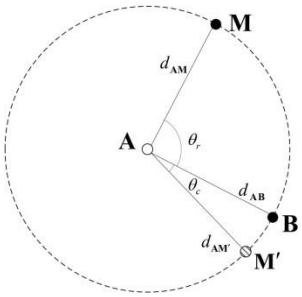

Figure 4.1: Illustration of our system model and the SDM attack

Optical signal-to-noise ratio (OSNR)

Optical Signal-to-Noise Ratio (OSNR) requirements, which largely depend on the ASE noise, tighten with the increasing complexity of modulation formats, where more complex and spectrally efficient modulation formats require higher OSNR to achieve acceptable Bit Error Rate (BER) values. The transmission reach limitation due to noise is also inversely proportional to the signal bit rate, i.e., signals with higher bit rates have a shorter reach.

Network scenario and assumptions

Routes and spectral resources to each demand, we apply the Spectrum-Spatial Allocation (SSA) algorithm from, aimed at minimizing the total network spectrum usage. The algorithm begins by sorting the demands in the descending order of their bit rates. For each demand, up to 30 candidate paths are computed, and associated with a modulation format and the number of required spectrum slices. The modulation format assignment follows the Distance- Adaptive Transmission (DAT) rule from aimed at maximizing the spectral

efficiency and minimizing the number of required regenerators. The number of slices required per candidate path is calculated as a function of demand bit rate and the applied modulation format.

Traffic disruption assessment

The jamming signal is considered to have power gain of 1 to 5 dB relative to the legitimate signals. We consider a worst-case attack scenario where the jamming signal traverses all fiber links in the topology. While in reality the spreading of the jamming signal can be thwarted at intermediate nodes, this assumption allows us to assess an upper bound on the possible network disruption caused by this type of attacks. For each demand, we verify whether the demand is disrupted by the attack or not, considering the reach limitations presented. A demand is considered as disrupted if its path length exceeds the maximum reach constraint imposed by the jamming attack.

Intra- and inter-channel

Investigates the intra- and inter-channel CrossTalk (XT) effects caused by the injection of high power jamming signals in WDM all-optical networks and shows their harmful effect to the performance of the optical channels. In [9], the authors propose approaches to decrease the overall damage caused by attacks through tailored, attack aware routing and/or wavelength assignment. The work proposes a design strategy that enhances the conventional Dedicated Path Protection (DPP) with attack-awareness. The above-mentioned studies show that physical-layer security can be enhanced while using the same amount of optical resources as conventional, resource-saving approaches. However, these works consider a WDM optical network where the damaging effects of jamming signals stay confined in a single fiber core. In SDM networks, signal interference among adjacent cores cannot be neglected, particularly in the presence of high-power jamming signals.

CONCLUSION

This paper investigates the extent of disruption caused by high-power jamming attacks to legitimate traffic in a SDM network. We quantify the attack-induced reduction of maximum transmission reach for different bit rates and modulation formats, as well as the resulting traffic losses at the network level. The study provides an insight into the safety margins that could be considered to mitigate traffic losses and increase SDM network security. The results show that the correct modulation format is crucial not only for the spectrum efficiency, as shown in the related works, but is also of utmost importance for the resiliency of demands against high-power jamming signal attacks.

Further studies are needed to understand how different optical network technologies affect the vulnerability to physical layer attacks. In particular, the migration from WDM to SDM optical networks may require new approaches to guarantee the security of the optical layer. Moreover, the different extent of disruptions can be observed depending on the considered traffic matrices and network topology, as well as the applied SSA algorithm. Finally, in addition to jamming signal attacks, other kinds of physical layer attacks need to be studied in order to offer high security and minimize the network vulnerability.

Future work

Further studies are needed to understand how different optical network technologies affect the vulnerability to physical layer attacks. In particular, the migration from WDM to SDM optical networks may require new approaches to guarantee the security of the optical layer. Moreover, the different extent of disruptions can be observed depending on the considered traffic matrices and network topology, as well as the applied SSA algorithm. Finally, in addition to jamming signal attacks, other kinds of physical layer attacks need to be studied in order to offer high security and minimize the network vulnerability.

REFERENCES

[1]. L. Zhu, C. Li, B. Li, X. Wang, and G. Mao, "Geographic routing in multilevel scenarios of vehicular ad hoc networks," IEEE Trans. Veh. Technol., 65(9), 7740–7753, 2016.

[2]. Y. Yao and N. Jiang, "Distributed wireless sensor network localization based on weighted search," Comput. Networks 86, 57–75, 2015.

[3]. L. Lin, Q. Sun, S. Wang, and F. Yang, "A geographic mobility prediction routing protocol for ad hoc uav network," in 2012 IEEE Globecom Workshops. IEEE, 1597–1602, 2012

[4]. P. Zhang, Z. Zhang, and A. Boukerche, "Cooperative location verification for vehicular ad-hoc networks," in IEEE International Conference on Communications. IEEE, 37–41, 2012

[5]. Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," IEEE Trans Parallel Distrib Syst 24(5), 938–950, 2013.

[6]. M. R. Ataei, T. Kunz, and A. H. Banihashemi, "Localization and location verification in non-homogeneous one-dimensional wireless adhoc networks," IEEE J Sel Areas Commun, 33(7), 1304– 1316, 2015.

[7]. T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," IEEE Wirel. Commun. 13(5), 2006.

[8]. Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie, "Secure localization and location verification in wireless sensor networks: a survey," J Supercomput, 64(3), 685–701, 2013.

[9]. K. Rasmussen, M. Srivastava et al., "Secure location verification with hidden and mobile base stations," IEEE Trans. Mob. Comput 7(4), 470–483, 2008.

[10]. R. Baker and I. Martinovic, "Secure location verification with a mobile receiver," in Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy. ACM, 2016, 35–46.

[11]. D. Liu, M.-C. Lee, and D. Wu, "A node-to-node location verification method," IEEE Trans Ind Electron, 57(5), 2010, 1526–1537.

[12]. S.-H. Fang, W.-H. Chang, Y. Tsao, H.-C. Shih, and C. Wang, "Channel state reconstruction using multilevel discrete wavelet transform for improved fingerprinting-based indoor localization," IEEE Sensors J., 16(21), 2016, 7784–7791.

[13]. Y. Xiong, N. Wu, H. Wang, and J. Kuang, "Cooperative detectionassisted localization in wireless networks in the presence of ranging outliers," IEEE Trans Commun, 65(12), 2017, 5165–5179.

[14]. G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Models and solutions for radio irregularity in wireless sensor networks," ACM Trans. Sens. Netw, 2(2), 2006, 221–262.

[15]. F. Yilmaz and M.-S. Alouini, "Sum of weibull variates and performance of diversity systems," in Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly. ACM, 2009, 247–252.

[16]. T. Mizuno, H. Takara, K. Shibahara, A. Sano, and Y. Miyamoto, "Dense space division multiplexed transmission over multicore and multimode fiber for long-haul transport systems," IEEE/OSA J. Lightwave Techn. 34(6), 2016. 1484–1493

[17]. W. Klaus, B. J. Puttnam, R. S. Luis, J. Sakaguchi, J.-M. D. Mendinueta, Y.Awari, and N. Wada, "Advanced space division multiplexing technologies for optical networks [invited]," IEEE/OSA J. Optical Commun. Netw. 9,(4), 2017, C1–C11.

[18]. M. Klinkowski, P. Lechowicz, and K. Walkowiak, "Survey of resource allocation schemes and algorithms in spectrally-spatially flexible optical networking," Opt. Switch. Netw. 27, 2017, 58–78.

[19]. K. Saitoh, T. Fujisawa, and T. Sato, "Design and analysis of weakly- and strongly-coupled multicore fibers," Proc. Photonic Netw.and Devices. NeTu2B. 5, 2017, 1 – 3.

[20]. J. Perelló, J. M. Gené, A. Pagès, J. A. Lazaro, and S. Spadaro, "Flex-grid/SDM backbone network design with inter-core XT-limited transmission reach," IEEE/OSA J. Opt. Commun.and Netw. 8(8), 2016, 540–552.

[21]. N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physicallayer security in evolving optical networks," IEEE Com. Mag, 54(8), 2016, 110–117.

[22]. Y. Peng, Z. Sun, S. Du, and K. Long, "Propagation of all-optical crosstalk attack in transparent optical networks," Opt. Eng, 50(8), 2011, 085 002.1–3.

[23]. M. Furdek, N. Skorin-Kapov, and L. Wosinska, "Attack-aware dedicated path protection in optical networks**,**" IEEE/OSA J. Lightwave Techn., 34(4), 2016, 1050–1061.

[24]. N. Skorin-Kapov, M. Furdek, R. A. Pardo, and P. P. Mariño, "Wavelength assignment for reducing in-band crosstalk attack propagation in optical networks: ILP formulations and heuristic algorithms," European Journal of Operational Research, 222(3), 2012, 418 – 429.

[25]. A. Muhammad, G. Zervas, and R. Forchheimer, "Resource allocation for space-division multiplexing: Optical white box versus optical black box networking," Journal of Lightwave Technology, 33(23), 2015, 4928–4941.

[26]. L. Zhang, N. Ansari, and A. Khreishah, "Anycast planning in space division multiplexing elastic optical networks with multi-core fibers," IEEE Communications Letters, 20(10), 2016, 1983–1986.

[27]. J. Zhu and Z. Zhu, "Physical-layer security in MCF-based SDMEONs: Would crosstalk-aware service provisioning be good enough?" IEEE/OSA J. Lightwave Techn, 35(22), 2017, 4826–4837.

[28]. R. J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, "Capacity limits of optical fiber networks," IEEE/OSA J. Lightwave Techn, 28, 2010, 662–701.

[29]. A. Sano et al., "409-tb/s + 409-tb/s crosstalk suppressed bidirectional mcf transmission over 450 km using propagation-direction interleaving," Opt. Express, 21(14), 2013, 16 777–16 783.

[30]. R. Go´scie´n, K. Walkowiak, and M. Klinkowski,"Distance-adaptive transmission in cloud-ready elastic optical networks," IEEE/OSA J. Opt. Commun. and Netw., 6,(10), 2014, 816–828.