International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 04, April-2018

A Review on Channel Aware Reputation System with Adaptive Detection for Attack-Tolerant Data Forwarding

K Naga Venkatesh, Y Raghu Vamsi, R Sakthi Prabha
Dept. of Electronics Communication Engineering,
Sathyabama Institute of Science and Technology,
Jeppiar Nagar, Rajiv Gandhi salai, Chennai-119.

Abstract: **- As a promising event monitoring and data gathering technique, wireless sensor network has been widely applied to both military and civilian applications. However, due to the lack of physical protection, sensor nodes are easily compromised by adversaries, making WSN vulnerable to various security threats. One of the most severe threats is selective forwarding attack, where the compromised nodes can maliciously drop a subset of forwarding packets to deteriorate the data delivery ratio of the network. It poses a good challenge to tell apart the malicious drop and traditional packet loss. During this paper, we propose a Channel-aware name System with adaptive detection threshold (CRS-A) to find selective forwarding attacks in WSNs. The CRS-A evaluates the information forwarding behaviors of sensor nodes, in step with the deviation of the monitored packet loss and also the calculable traditional loss. To optimize the detection accuracy of CRS-A, we tend to in theory derive the best threshold for forwarding analysis, that is adaptive to the time varied channel condition and also the calculable attack chances Of compromised nodes.**

Index Terms— Wireless Sensing Element Network, Selective Forwarding Attack, Reputation system, packet dropping, channel-aware, is routing.

INTRODUCTION:

Wireless sensor networks (WSN's) are fault-tolerant, scalable and dynamic in nature. Sensor nodes are of low cost and easy to install. Sensor nodes are self-controlled in nature. Sensor nodes have short life span, limited memory and capacity of computation is low. These nodes gather information from their surrounding and send it to the user-controlled systems which are base stations (BS).sensor nodes are used for both military surveillances and civilian applications. Sensor nodes are also used to detect natural disasters like earth quakes, tsunamis and volcanic reactions. These sensor nodes are deployed in the sensor field. However, due to the lack of physical protection, sensor nodes are easily compromised, making WSN vulnerable to various security threats. One of the most common threats is selective forwarding attack, where the compromised nodes can maliciously drop a subset of forwarding packets to deteriorate the data delivery ratio of the network. Since WSNs are generally deployed in open areas (e.g., primeval forest), the unstable wireless channel and medium access collision can cause remarkable normal packet losses. The selective forwarding attacks are concealed by the normal packet losses, complicating the selective forwarding attack detection. Therefore, it is challenging to detect the selective forwarding attacks and improve the network performance.During each evaluation period, sensor nodes calculate the normal packet loss rates between themselves and their neighbouring nodes, and assume the estimated packet loss rates to evaluate the forwarding behaviours of its neighbours along the data forwarding path. The sensor nodes misbehaving in data forwarding are taken into consideration with reduced reputation values by CRS-A. When the reputation value of a senor node is below than critical value, it would be identified as a compromised node by CRS-A. Compared to our previous work, this paper has the following enhancements and new contributions.To improve detection accuracy and packet delivery ration we propose the technique named as CRS-A. In CRS-A, each sensor node maintains a reputation table to evaluate the long-term forwarding behaviours of its neighbouring nodes. The essence of CRS-A is to dynamically update the reputation table based on the forwarding behaviour evaluation for the neighbouring nodes, by taking the normal packet loss rate into consideration.

1.2 Literature Survey:

1)SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks ----->Yih-Chun Hu, David B. Johnson and Adrian Perrig.

–In this paper, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV).

Pros and cons:
SEAD is efficient and can be used in networks of computation- and bandwidth-constrained nodes. SEAD actually outperforms DSDV-SQ in terms of packet delivery ratio. But the self-advertising routes of the nodes are not included and DSDV is not behaving like a path vector routing protocol.

2) On Intrusion Detection and Response for Mobile Ad Hoc Networks ----->James Parker, Jeffrey Under coffer, John Pinkston, and Anupam Joshi

– We present network intrusion detection (ID) mechanisms that rely upon packet snooping to detect aberrant behavior in mobile ad hoc networks. Our extensions, which are applicable to several mobile ad hoc routing protocol, offer two response mechanisms, passive - to singularly determine if a node is intrusive and act to protect itself from attacks, or active - to collaboratively determine if a node is intrusive and act to protect all of the nodes of an adhoc cluster.

Pros and cons:
A dropping of the packet can easily be recognized and logged. The implementation of both the Passive and Active ID algorithms in GloMoSim led to a number of parameters that can be adjusted. But

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 04, April-2018

the performance is not greatly enhanced and the node density is not determined.

3)An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in WSNs----->Kejun Liu, Jing Deng, Pramod K. Varshney and KashyapBalakrishnan.

– In this paper, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their diverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path.

Pros and cons:

Compared with other approaches to combat the problem, such as the overhearing technique, the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers. The 2ACK scheme can be used as an add-on technique to routing protocols such as DSR in WSNs. But, the knowledge of topology of the 2-hop neighborhood may be used. In addition, the 2ACK scheme can only work in managed WSNs (as compared to open WSNs).

4) Anonymous Communications in Mobile Ad Hoc Networks---

2	On Intrusion Detection and Response for Mobile Ad Hoc Networks	James Parker, Jeffrey Under coffer, John Pinkston, and Anupam Joshi	A dropping of the packet can easily be recognized and logged. The implementation of both the Passive and Active ID algorithms in GloMoSim led to a number of parameters that can be adjusted	Performance is not greatly enhanced and the node density is not determined.
3	An Acknowledg ment-Based Approach for the Detection of Routing Misbehavior in WSNs	Kejun Liu, Jing Deng, Pramod K. Varshney and KashyapB alakrishna n.	The 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers	The knowledge of topology of the 2-hop neighborhood may be used. In addition, the 2ACK scheme can only work in managed WSNs
4	Anonymous Communicat ions in Mobile Ad Hoc Networks	Yanchao Zhang, Wei Liu and Wenjing Lou.	MASK provides strong sender and receiver anonymity, the relationship anonymity between senders and receivers, the unlocatability of mobile nodes, and the intractability of packet flows under a strong adversarial model	The routing information is not authenticated in the current design of MASK.

>Yanchao Zhang, Wei Liu and Wenjing Lou.

–In this paper, author proposes a novel anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks. The cryptographic concept of pairing explains the anonymous neighbourhood authentication protocol which is done by allowing neighboring nodes to authenticate each other without revealing their identities.

Pros and cons:

A pairing-based anonymous on-demand routing protocol MASK is which provides strong sender and receiver anonymity, the relationship anonymity between senders and receivers, the unlocatability of mobile nodes, and the intractability of packet flows under a rather strong adversarial model but the routing information is not authenticated in the current design of MASK.

5)On Flow Correlation Attacks and Countermeasures in Mix Networks---->Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao.

–In this paper, author focus on a particular class of traffic analysis attack, flow correlation attacks, by which an adversary attempts to analyze the network traffic and correlate the traffic input link at a mix with output link of the same mix.

Pros and cons:

Analysing of mix networks was done in terms of their effectiveness in providing anonymity and quality-of-service and it shows that it can achieve a guaranteed low detection rate while maintaining high throughput for normal payload traffic but unlinkability alone is not enough in hostile environments like battlefields as important information like packet type is still available to attackers. Then a passive attacker can mount traffic analysis based on packet type.

SURVEY TABLE:

S. NO	TITLE	AUTHOR	OBSERVATION	DRAWBACK
1	SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks	Yih-Chun Hu, David B. Johnson and Adrian Perrig.	SEAD is efficient and can be used in networks of computation- and bandwidth-constrained nodes. SEAD actually outperforms DSDV-SQ in terms of packet delivery ratio	Self-advertising routes of the nodes are not included and DSDV is not behaving like a path vector routing protocol

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 04, April-2018

5	On Flow Correlation Attacks and Countermeasures in Mix Networks	Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao.	Analysing of mix networks was done in terms of their effectiveness in providing anonymity and quality-of-service and it shows that it can achieve a guaranteed low detection rate while maintaining high throughput for normal payload traffic	Unlinkability alone is not enough in hostile environments like battlefields as important information like packet type is still available to attackers. Then a passive attacker can mount traffic analysis based on packet type

CONCLUSION:

In this paper, we have proposed a channel-aware reputation system with adaptive detection threshold to identify selective forwarding attacks in WSNs. CRS-A evaluates the deviation between the estimate normal packet loss and monitored packet loss for finding forwarding behaviors. For adaptive time-varied channel condition and the attack probability of compromised nodes we have further derived the optimal evolution threshold of CRS-A.

REFERENCES:

[1] I. Butun, S. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Commun. Surv.&Tutor., vol. 16, no. 1, pp. 266–282, 2014.

[2] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," IEEE Trans. Commun., vol. 61,no. 12, pp. 5103–5113, 2013.

[3] Y. Zhang, L. Lazos, and W. Kozma, "Amd: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mob. Comput.,prePrints, published online in Sept. 2013.

[4] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, "A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks," Comput. Commun.vol. 35, no. 17, pp. 2125–2137, 2012.

[5] X. Liang, X. Lin, and X. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," IEEE Trans. Parallel Distr. Sys., vol. 25, no. 2, pp. 310–320, 2014.

[6] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Sacrm: Social aware crowdsourcing with reputation management in mobile sensing," Computer Commun., vol. 65, no. 15, pp. 55–65, 2015.

[7] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting channel-aware reputation system against selective forwarding attacks in wsns," in Proc. IEEE GLOBECOM, 2014, pp. 330–335.

[8] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting mobile crowdsourcing for pervasive cloud services: challenges and solutions," IEEE Commun. Mag., vol. 53, no. 3, pp. 98–105, 2015

[9] R.Sakthi prabha, BIECC- an efficient cryptographic scheme for authenticate false data injection over wireless sensor networks International Journal of Applied Engineering Research ISSN 0973-4562 Vol 10, Number 2 pp. 3557-3565(2015)

[10] J. Tang, Y. Cheng, and W. Zhuang, "Real-time misbehavior detection in ieee 802.11-based wireless networks: An analytical approach," IEEE Trans. Mob. Comput., vol. 13, no. 1, pp. 146–158, 2014.

[11] T. Liu and A. E. Cerpa, "Data-driven link quality prediction using link features," ACM Transactions on Sensor Networks (TOSN), vol. 10, no. 2, p. 37, 2014.