© 2018 IJSRSET | Volume 4 | Issue 7 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Designing Security System for Ring Topology in WSN

Pooja Tekade, Prof. Nutan Dhande
Department of Computer Science and Engineering ACE Nagthana Wardha Maharashtra, India

ABSTRACT

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 to accurately compute aggregates (e.g., predicate count or sum). However, this aggregation framework does not address the problem of false sub-aggregate 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.

Keywords: WSN, Data Aggregation,Attack Resilient

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. 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.

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" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as

energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

II. RELATED WORK

In this section, we provide a brief background study on different types of MANET IDS based on their detection mechanism and modes of operation. We then discuss about various intrusion detection issues in MANETs and analyze the related works which have been categorized into non-game theory based and game theory based. Finally, the drawbacks associated with the related works have been listed out which provides us with the motivation for our work to address them.

1. EAACK – a secure intrusion-detection system for MANETs

Authors: E.M. Shakshuki, N. Kang, T.R. Sheltami

Shakshuki et al. [18] proposed an IDS named Enhanced Adaptive Acknowledgment (EAACK) for MANETs. Their scheme requires all acknowledgment packets to be digitally signed by its sender and verified by its receiver. They used DSA and RSA as digital signatures and showed that their scheme is able to detect wide range of attacks. However, the drawback of their scheme is the requirement to digitally sign all the acknowledgments which increases computational overhead.

2. Mitigating routing misbehavior in mobile ad hoc networks

S. Marti, T.J. Giuli, K. Lai, M. Baker

Marti et al. [32] proposed an IDS scheme for MANET which consists of two different modules, viz. the Watchdog and the Pathrater. In this scheme, the Watchdog acts as an IDS for the MANET and detects malicious node behaviors in the network by promiscuously listening to its next hop's transmission. If the Watchdog notices that its immediate next node fails to forward the packet within a given period of time then it increments the node's failure counter. If the failure counter of the monitored node exceeds a threshold value then the Watchdog reports the node as misbehaving. The Pathrater is then employed to inform the routing protocol to avoid the reported nodes for further data transmission. The drawback of this scheme is that it requires continuous monitoring by the Watchdog for detecting intrusions.

3. An acknowledgment-based approach for the detection of routing misbehavior in MANETs

K. Liu, J. Deng, P.K. Varshney, K. Balakrishnan

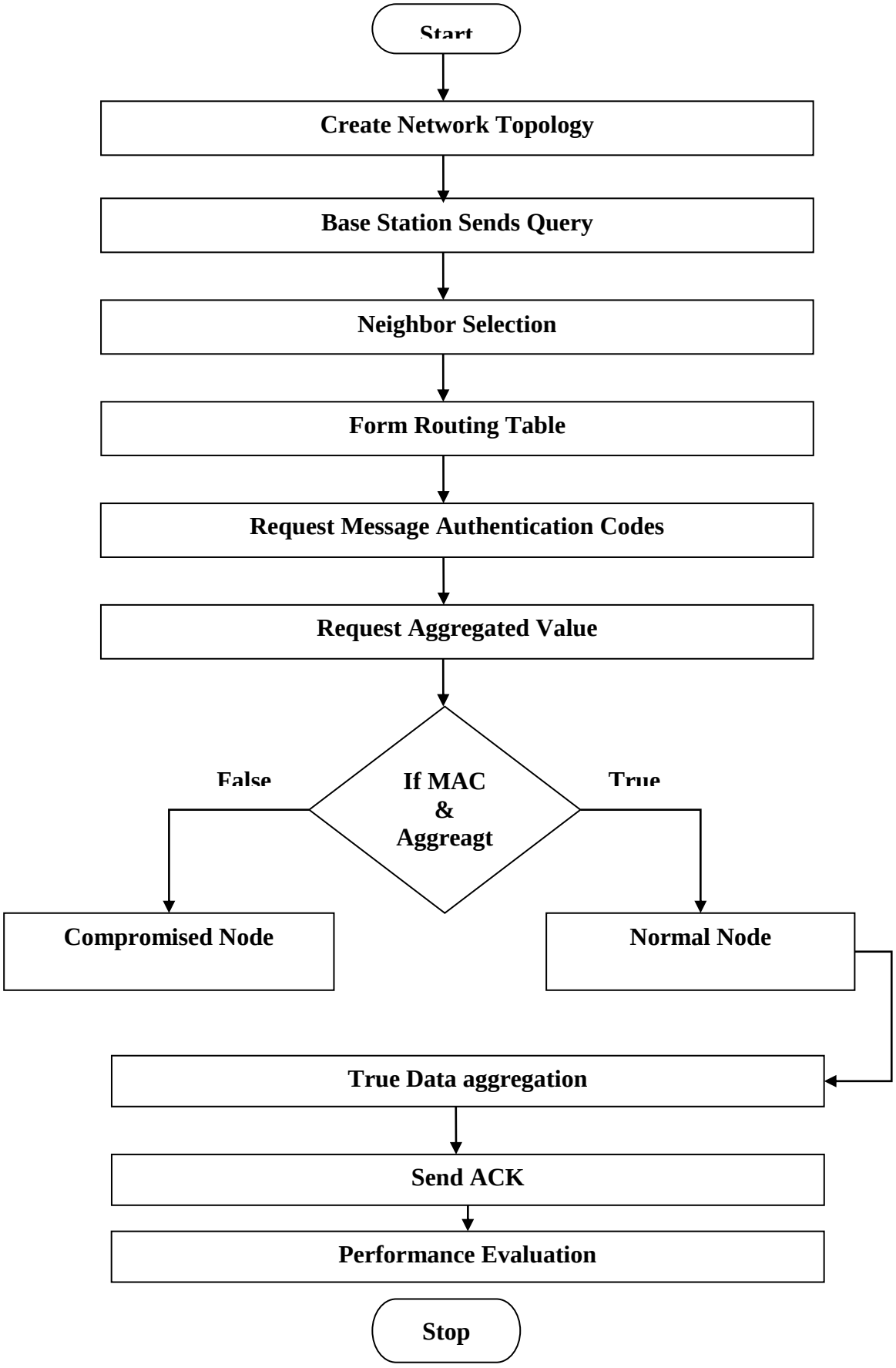
Lui et al. [17] proposed a TWOACK MANET IDS scheme which requires every data packets transmitted over three consecutive nodes along the source to the destination path to be acknowledged. Every node along the route has to send back an acknowledgment packet to the node that is two hop counts away from it in the route. The arrival of TWOACK packet at first node X (in the three consecutive nodes along the route) indicates a successful transmission of packet from node X to node Z via the intermediate node Y. However, if this TWOACK packet is not received within a given predefined time interval, both nodes Y and Z are reported as malicious. The drawback of this scheme is that it introduces a routing overhead due to frequent TWOACK packet generation.

4. Energy efficient learning solution for intrusion detection in Wireless Sensor Networks

S. Misra, P. Krishna, K. Abraham

Misra et al. [33] proposed a distributed self-learning, energyaware and low complexity protocol for intrusion detection in wireless sensor network. Their protocol uses the stochastic Learning Automata (LA) on packet sampling mechanism to obtain an energy efficient IDS. They showed that their approach was successful in detecting and removing malicious packets from the WSN. The drawback of this scheme is that the LA needs multiple rounds of learning before it becomes efficient.

III. PROPOSED METHODOLOGY



IV. SETTING UP NETWORK MODEL

Our first module is setting up the network model. We consider a large-scale, homogeneous sensor network consisting of resource-constrained sensor nodes. Analogous to previous distributed detection approaches; we assume that an identity-based public-key cryptography facility is available in the sensor network. Prior to deployment, each legitimate node is allocated a unique ID and a corresponding private key by a trusted third party. The public key of a node is its ID, which is the essence of an identity-based cryptosystem. Consequently, no node can lie to others about its identity. Moreover, anyone is able to verify messages signed by a node using the identity-based key. The source nodes in our problem formulation serve as storage points which cache the data gathered by other nodes and periodically transmit to the sink, in response to user queries. Such network architecture is consistent with the design of storage centric sensor networks

Falsifying the local value:

A compromised node C can falsify its own sensor reading with the goal of influencing the aggregate value. We assume that if a node is compromised, all the information it holds will be compromised. We conservatively consider that all malicious nodes can collude or can be under the control of a single attacker. We use a Byzantine fault model, where the adversary can inject any message through the compromised nodes. Compromised nodes may behave in arbitrarily malicious ways, which means that the sub-aggregate of a compromised node can be arbitrarily generated. However, we assume that the attacker does not launch DoS attacks, e.g., the multi-hop flooding attacks with the goal of making the whole system unavailable.

Computing Sum Despite Attacks:

In this module, we develop an attack-resilient protocol which enables BS to compute the aggregate despite the presence of the attack. We observe that, in general, BS can verify the final synopsis if it receives one valid MAC for each '1' bit in the synopsis. In fact, to verify a particular '1' bit, say bit i , BS does not need to receive authentication messages from all of the nodes which contribute to bit i . As an example, more than half of the nodes are likely to contribute to the leftmost bit of the synopsis, while to verify this bit, BS needs to receive a MAC only from one of these nodes.

V. CONCLUSION

We 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. We presented an attack-resilient computation algorithm which would guarantee the successful computation of the aggregate even in the presence of the attack.

VI. REFERENCES

[1]. A. Mishra, K. Nadkarni, A. Patcha, Intrusion detection in wireless Ad-hoc networks, IEEE Wirel. Commun. 11 (1) (2004) 48-60.

[2]. Y. Zhang, W. Lee, Y.-A. Huang, Intrusion detection techniques for mobile wireless networks, Wirel. Netw. 9 (5) (2003) 545-556.

[3]. M. La Polla, F. Martinelli, D. Sgandurra, A survey on security for mobile devices, IEEE Commun. Surv. Tutor. 15 (1) (2013) 446-471.

[4]. F. Anjum, P. Mouchtaris, Intrusion Detection Systems, John Wiley & Sons, Inc., 2006.

[5]. P. Brutch, C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, in: Proceedings of Symposium on Applications and the Internet Workshops, 2003, pp. 368-373.

[6]. Y.-C. Hu, A. Perrig, D. Johnson, Ariadne: a secure on-demand routing protocol for ad-hoc networks, Wirel. Netw. 11 (1-2) (2005) 21-38.

[7]. S. Bu, F. Yu, X. Liu, P. Mason, H. Tang, Distributed combined authentication and

intrusion detection with data fusion in high-security mobile ad hoc networks, IEEE Trans. Veh. Technol. 60 (3) (2011) 1025-1036.

[8]. Z. Fadlullah, H. Nishiyama, N. Kato, M. Fouda, Intrusion detection system (IDS) for combating attacks against cognitive radio networks, IEEE Netw. 27 (3) (2013) 51-56.

[9]. Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, 2000, pp. 275-283.

[10]. T. Anantvalee, J. Wu, A survey on intrusion detection in Mobile Ad Hoc Networks, in: Wireless Network Security, Signals and Communication Technology, Springer, 2007, pp. 159-180.

[11]. A. Mitrokotsa, C. Dimitrakakis, Intrusion detection in MANET using classification algorithms: the effects of cost and model selection, Ad Hoc Netw. 11 (1) (2013) 226-237.

[12]. C. Xenakis, C. Panos, I. Stavrakakis, A comparative evaluation of intrusion detection architectures for mobile ad hoc networks, Comput. Secur. 30 (1) (2011) 63-80.

[13]. I. Butun, S. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 266-282.

[14]. R. Mitchell, I. Chen, Effect of intrusion detection and response on reliability of cyber physical systems, IEEE Trans. Reliab. 62 (1) (2013) 199-210.

[15]. A. Patel, M. Taghavi, K. Bakhtiyari, J.C. Jnior, An intrusion detection and prevention system in cloud computing: a systematic review, J. Netw. Comput. Appl. 36 (1) (2013) 25-41.

[16]. M. Ficco, L. Romano, A generic intrusion detection and diagnoser system based on complex event processing, in: First International Conference on Data Compression, Communications and Processing, 2011, pp. 275-284.

[17]. K. Liu, J. Deng, P.K. Varshney, K. Balakrishnan, An acknowledgment-based approach for the detection of routing misbehavior in MANETs, IEEE Trans. Mob. Comput. 6 (5) (2007) 536-550.

[18]. E.M. Shakshuki, N. Kang, T.R. Sheltami, EAACK-a secure intrusion-detection system for MANETs, IEEE Trans. Ind. Electron. 60 (3) (2013) 1089-1098.

[19]. Y. Liu, C. Comaniciu, H. Man, A Bayesian game approach for intrusion detection in wireless ad hoc networks, in: Proceedings of the 2006 Workshop on Game Theory for Communications and Networks, ACM, 2006.

[20]. A. Agah, S. Das, K. Basu, M. Asadi, Intrusion detection in sensor networks: a non-cooperative game approach, in: Proceedings of Third IEEE International Symposium on Network Computing and Applications, 2004, pp. 343-346.

[21]. T. Alpcan, T. Basar, A game theoretic approach to decision and analysis in network intrusion detection, in: Proceedings of 42nd IEEE Conference on Decision and Control, 2003, pp. 2595-2600.

[22]. Y. Huang, W. Lee, A cooperative intrusion detection system for ad hoc networks, in: Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003, pp. 135-147.

[23]. M. Kodialam, T. Lakshman, Detecting network intrusions via sampling: a game theoretic approach, in: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, vol. 3, 2003, pp. 1880-1889.

[24]. A. Mas-Colell, M. Whinston, J. Green, Microeconomic Theory, New York, Oxford University Press, 1995.

[25]. T. Issariyakul, E. Hossain, Introduction to Network Simulator NS2, 1st ed., Springer Publishing Company, Incorporated, 2008.

[26]. P. Barford, J. Kline, D. Plonka, A. Ron, A signal analysis of network traffic anomalies, in: Proceedings of the 2nd ACM SIGCOMM

Workshop on Internet Measurement, 2002, pp. 71-82.

[27]. A. Lakhina, M. Crovella, C. Diot, Mining anomalies using traffic feature distributions, Comput. Commun. Rev. 35 (4) (2005) 217-228.

[28]. J. Dickerson, J. Dickerson, Fuzzy network profiling for intrusion detection, in: 19th International Conference of the North American Fuzzy Information Processing Society, 2000, pp. 301-306.

[29]. A. Valdes, K. Skinner, Adaptive, model-based monitoring for cyber attack detection, in: Recent Advances in Intrusion Detection, vol. 1907, 2000, pp. 80- 93.

[30]. M. Roesch, Snort-lightweight intrusion detection for networks, in: Proceedings of the 13th USENIX Conference on System Administration, 1999, pp. 229-238.

[31]. R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, et al., Specificationbased anomaly detection: a new approach for detecting network intrusions, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 265-274.

[32]. S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, 2000, pp. 255- 265.

[33]. S. Misra, P. Krishna, K. Abraham, Energy efficient learning solution for intrusion detection in Wireless Sensor Networks, in: Second International Conference on Communication Systems and Networks, 2010, pp. 1-6.

[34]. F. Haddadi, M. Sarram, Wireless intrusion detection system using a lightweight agent, in: Second International Conference on Computer and Network Technology, 2010, pp. 84-87.

[35]. M. Mohanapriya, I. Krishnamurthi, Modified DSR protocol for detection and removal of selective black hole attack in MANET, Comput. Electr. Eng. 40 (2) (2014) 530-538.