IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IV (Sep – Oct. 2014), PP 14-17
www.iosrjournals.org

A Novel Approach for intrusion Detection in Heterogeneous Wireless Sensor Networks using multipath Routing

Suman Jyothula
Assistant Professor, CSE Dept., India

Abstract: *The key concept of my redundancy management is to exploit the tradeoff between energy consumption vs. to the gain of reliability, timeliness, and also security for maximizing the system useful lifetime in this paper I am proposing to explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each and every with some different implications for energy, security and also reliability, and the investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. Intrusion detection is a security mechanism which is used to identify those who are trying to break and misuse the system without authorization and also those who have legitimate access but misusing their privileges.*

Keywords: *Cyber physical system, Heterogeneous Wireless Sensor Networks, Intrusion detection system, Multipath routing.*

I. Introduction

Intrusion detection system (IDS) design for CPSs has attracted considerable attention. Detection techniques in general can be classified into three types: the signature based, the anomaly based, and the specification based techniques. In the area of signature based IDS techniques, an IDS for CPSs that tests an automated transform from XML parole to Snort signature in an electricity distribution laboratory. An IDS for CPSs that takes a multi trust hybrid approach using signature based detection and traffic analysis. My work is different from these studies in that I use specification based detection rather than signature based detection to deal with unknown attacker patterns.

Wireless sensor networks are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to some limited resources, a WSN must not be only satisfied by the application specific QoS requirements such as reliability, timelines and also security, but also minimize the consumption of energy to prolong the system's useful lifetime. Where the tradeoff between the energy consumption vs. reliability gain with that of the goal to maximize the WSN system lifetime has been well explored in the literature. However, here no before work exists to consider that the tradeoff in the presence of malicious attackers. The Intrusion detection system monitors the activities of the system, analyze the activities to determine, any of the activity is violating the security rules. Once an IDS determines that an unusual activity or an event that is known to cause an attack happens, it then generates an Introduction.

Thus, very likely the system would employ an intrusion detection system (IDS) with the goal to detect and remove malicious node .Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. It satisfies the energy consumption through turn off the sensor nodes for period of time to save energy. The basic idea is that the probability of at least one path reaching the sink node or base station increases as I have more paths doing data delivery. While the most priority prior research focused on using multipath routing to improve the reliability, some attention has to be paid for using multipath routing to tolerate insider attacks.

A cyber physical system (CPS) typically comprises sensors, actuators, control units, and physical objects for controlling and protecting a physical infrastructure. Because of the dire consequence of a CPS failure, protecting a CPS from malicious attacks is of paramount importance. In this paper, we address the reliability issue of a CPS designed to sustain malicious attacks over a prolonged mission period without energy replenishment. A CPS often operates in a rough environment wherein energy replenishment is not possible, and nodes may be compromised (or captured) at that times. Thus, an intrusion detection and response system (IDRS) must be detected as malicious nodes without unnecessarily wasting energy to prolong the system lifetime.

Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic possibility is that the probability of at least one path reaching the sink node or base station increases as I have more paths doing data delivery. While the most priority prior research focused on using multipath routing to improve reliability some attention has been paid to using multipath routing to tolerate insider attacks. Coming to these studies, however, largely (highly) ignored the tradeoff between QoS gain vs. energy consumption with which it can adversely shortens the system lifetime.

The tradeoff issue between energy consumption vs. QoS gain becomes much more complicated when inside attackers are present as a path may be broken when a malicious node is on the path. Where this is especially the task in heterogeneous WSN (HWSN) environments in which the CH nodes wills to take a more critical role in collecting/gathering and routing sensing the data. Thus, the very likely on the system would employ an intrusion detection system (IDS) with the goal to detect and remove malicious nodes. While the literature is abundant in intrusion detection techniques for WSNs, the issue of how often intrusion detection should be invoked for energy reasons in order to remove potentially malicious nodes so that the system lifetime is maximized (say to prevent a Byzantine failure) is largely unexplored. Thus the issue is especially been critical for the energy constrained WSNs designed to stay alive for a long mission time.

II. Architecture

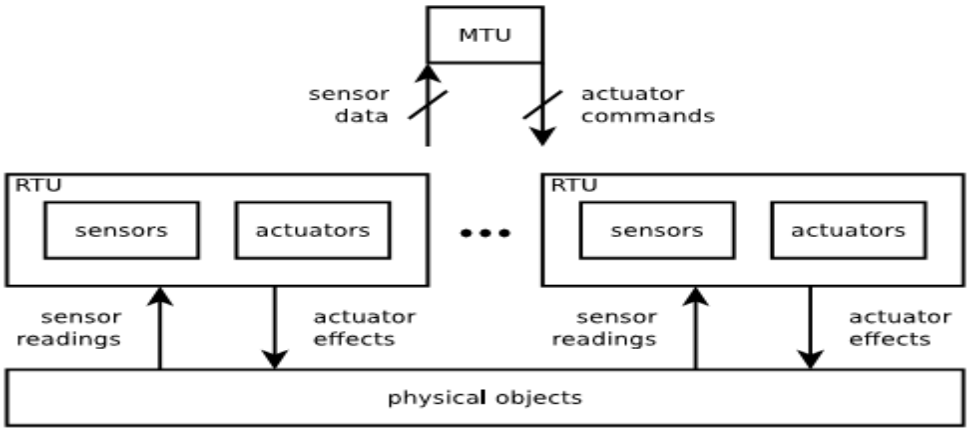

Fig.1 CPS architecture

Fig. 1 contextualizes our reference CPS which comprises 128 sensor-carried mobile nodes, a control unit, and physical objects for controlling and protecting a physical infrastructure. At present the mobile nodes are very Capable of sensing physical environments, and also as well as actuating and controlling the underlying physical objects in the CPS. They function as sensors and actuators, where the each carrying sensors for sensing physical phenomena, as well as actuating devices for controlling physical objects. The CPS literature which identifies these kind of mobile nodes as RTUs. Sitting on top of these mobile nodes is a control unit which receives sensing data from the mobile nodes and determines actions to be performed by individual nodes or a group of mobile nodes. This triggers their actuating devices to control and protect the physical objects in the CPS. I exemplify a number of applications to which our reference CPS can apply.

1) **Disaster recovery** (say after an earthquake) might involve a group of mobile nodes with motion and video sensing and actuating capabilities cooperating under the control of a disaster corrective control unit to protect and recover physical objects (e.g., people or a physical infrastructure).

2**) Emergency rescue** (say a burning building) may require a group of mobile fighters equipped with motion and video sensing and fighting capabilities cooperating under the control of a control unit to rescue in the physical objects (e.g., people are being trapped or seized).

3**) Military patrol** (combat or reconnaissance) might consist of a group of mobile patrol nodes equipped with motion sensing and fighting capabilities cooperating under the control of a control unit to protect and control physical objects (e.g., geographic areas or critical resources).

4) **Pervasive healthcare** might use a group of mobile medical personnel equipped with motion and video sensing and actuating capacities cooperating under the control of a control unit to protect and provide healthcare to physical objects (e.g., patients or medical devices).

5) **Unmanned aircraft systems** might consist of a group of unmanned aerial vehicles equipped with sensing and aircraft fighting capabilities cooperating under the control of a remote control unit to control and protect physical objects (e.g., geographic areas).

III. Existing Work

Over the past few years, many protocols exploring the tradeoff between energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. In [9], here the optimal communication range and also communication mode were described to maximize the HWSN lifetime. In [10], the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. The

consideration of a hierarchal HWSN with CH nodes definitely having larger energy and also processing capabilities than a normal SNs.

Where the solution is to be formulated as an optimization problem in balancing the energy consumption across all nodes with their roles. Here in either works that cited above, no consideration was given to the existence of malicious nodes. In [7], the authors considered a two-tier HWSN with the objective of maximizing network lifetime while fulfilling power management and coverage objectives determined the optimal density ratio of the two tier's nodes to always maximize the systems lifetime. Relative to [10] my work also considers heterogeneous nodes with different densities and capabilities. However, my work considers the presence of malicious nodes and explores the tradeoff between energy consumption vs. QoS gain in both of the security and reliability is always to maximize the systems lifetime.

In the context of secure multipath routing for intrusion tolerance, [11] provides an excellent survey in this topic. In [5] the authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks.

.

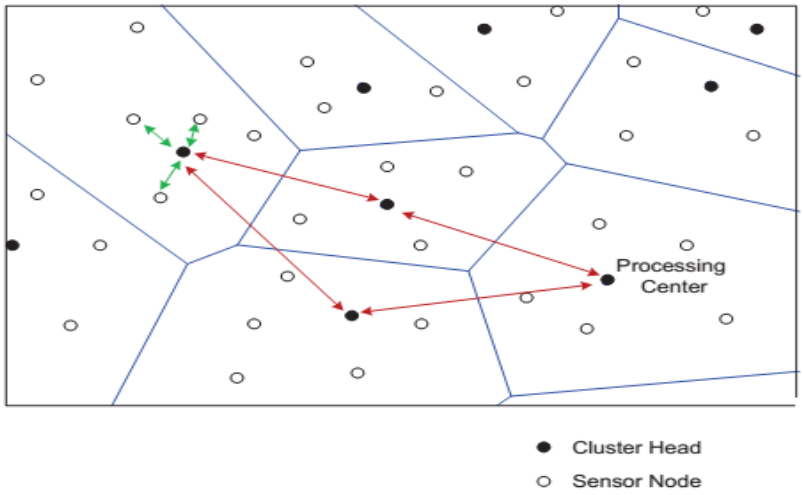

Fig.2:source & path redundancy for a HWSN

The basic idea is to use overhearing to avoid sending packets to malicious nodes. In [4] that the authors here considered a disjoint multipath routing protocol to tolerate intrusion using multiple disjoint paths in WSNs. my work also uses multipath routing to tolerate intrusion. However, I specifically consider energy being consumed for intrusion detection, and both CHs and SNs can be compromised for lifetime maximization. In [3] a randomized dispersive multipath routing protocol is proposed to avoid black holes.

IV. Proposed Method

In this paper the proposing system is to explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each and every with some different implications for the energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. And also proposing smart and insidious attackers which can perform more targeted attacks, which then captures certain strategic nodes with higher probability, here the alternate between benign and malicious behavior and collude with other attackers to avoid intrusion detection.

A HWSN comprises sensors of different capabilities. I have considered two types of sensors: CHs and SNs. CHs are superior to the SNs in energy and computational resources. I have used ECH in it and ESN in it to denote the initial energy levels of CHs and SNs, with respectively.

While my approach can be applied to any shape of the operational area, for analytical tractability, I assume that the deployment area of the HWSN is of size A2 CHs and SNs are distributed in the operational area. To ensure coverage, I assume that CHs and SNs are deployed randomly and distributed according to homogeneous spatial Poisson processes with intensities λCH and λSN, respectively, with $\lambda CH < \lambda SN$. The radio ranges used by CH and SN transmission is denoted by rCH and rSN, with respectively.

The radio range and the transmission power of both CHs and SNs are dynamically adjusted throughout the system lifetime to maintain the connectivity between CHs and between to SNs. where any communication between two nodes with a distance greater than single hop radio range between them would require multichip routing. Due to the limited energy, a packet is to be sent hop by hop without using any acknowledgment or retransmission.

Therefore an Intrusion Detection System (IDS) is required to monitor the network, detects anomalies and notifies other nodes to avoid or punish the misbehaving node.. The proposed IDS is for multi-hop ad-hoc wireless networks, which detects nodes misbehavior and anomalies using simple rules and with the help of a special node called monitor node. There will be more than one monitor node in the network and they will be periodically elected using an Election algorithm.

V. Conclusion

Finally I conclude that my approach is more efficient and secure in detecting intrusions by analyzing the routing paths and packet count techniques.

References

[1] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks,"IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, 2004.
[2] E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," IEEE Trans. Mobile Comput.,vol.5,no. 6, pp. 738–754, 2006.
[3] I. R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive fault-tolerant
[4] QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks,"IEEE Trans. Dependable Secure Computing, vol. 8, no. 2, pp. 161–176, 2011.
[5] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," inProc. 2005 IEEE Conf. Computer Commun., vol. 2, pp. 878–890.
[6] H. M. Ammari and S. K. Das, "Promoting heterogeneity, mobility, and energy-aware Voronoi diagram in wireless sensor networks,"IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 7, pp. 995–1008, 2008.
[7] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," inProc. 2005 IEEE Veh. Technol. Conf.,pp. 2528–2532.
[8] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," IEEE Wireless Commun. Mag., vol. 14, no. 5, pp. 560–563, 2007.
[9] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 2007 European Wireless Conf.
[10] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks,"IEEE Trans. Reliab., vol. 59, no. 1, pp. 231–241, 2010.
[11] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L.B. Ruiz, and H. C. Wong, "Decentralizedintrusion detection in wireless sensor networks," inProc. 2005 ACM Workshop Quality Service Security Wireless Mobile Netw.

ABOUT AUTHOR

SUMAN JYOTHULA received the B.Tech degree in 2009 from JNTU, Kakinada, and the M.E degree in 2011 from Sathyabama University; He is currently working toward the Ph.D. degree in Acharya Nagarjuna University. His research interests include Networking, Cloud Computing, and cryptography.