Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.255 – 260

RESEARCH ARTICLE

Trust Based Voting Scheme and Optimal Multipath Routing for Intrusion Tolerance in Wireless Sensor Network

[1]P.PRIYADHARSHINI, [2]C.ANOOR SELVI
[1]M.E/CSE, [2]A.P/CSE
[1,2]V.S.B Engineering College, Karur, TamilNadu
[1] priyadharshini.soft06@gmail.com, [2] sri.anu500@gmail.com

Abstract—**Wireless sensor networks (WSNs) deployed in unattended environment energy recharging is difficult. WSN satisfy application specific QoS requirements i.e., reliability, timeliness, security and minimize energy consumption to prolong system useful lifetime with limited resources. The drawbacks of existing work include redundancy management scheme that did not addresses heavy query traffic. Ambiguity in multi-path routing decision is due to higher level of intrusion tolerance rate. The proposed work presented Trust Based Neighbor Weighted Voting Scheme to strengthen intrusion detection in WSN. It evaluates the dynamic radio range of neighbor nodes. Weight threshold is evaluated for marking the sensor node as normal node and malicious node. It discards the communication of internal malicious node by identifying lower weight votes of corresponding sensor node. It governs the best WSN settings in terms of redundancy level used for outsource multipart routing number of weighted votes intrusion invocation interval. WSN lifetime is maximized with trust based weighted voting and handles concurrent higher query traffic.**

Keywords—Wireless Sensor Network; selective capture multipath routing; intrusion detection; lifetime maximization

I. INTRODUCTION

Wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must minimize energy consumption to prolong the system useful lifetime, while satisfying the application specific QoS requirements such as reliability, timeliness and security. This is especially a critical issue in military or mission-critical WSN applications. Sensor nodes (SNs) close to the base station (BS) are more critical in gathering and routing sensing data. In the literature, various schemes have been designed for preserving critical SNs from energy exhaustion so as to prolong the system lifetime; however, how to counter selective capture.

We propose and analyze an adaptive network management algorithm with 3 countermeasures to counter selective capture: (1) dynamic radio range adjustment; (2) multisource multipath routing for intrusion tolerance; and (3) voting-based intrusion detection. We develop a probability model to reveal the tradeoff between energy consumption vs. reliability and security gain with the goal to maximize the lifetime of a query-based WSN. More specifically, we analyze the optimal amount of redundancy for multipath routing and the best intrusion detection settings for detection strength under which the lifetime of a query-based WSN is maximized in the presence of selective capture.

II. RELATED WORK

The framework is designed by I. R. Chen et al., (2011) adaptive fault tolerant quality of service (QoS) control algorithms based on hop-by-hop data delivery utilizing “source” and “path” redundancy, with the goal to satisfy application QoS requirements while prolonging the lifetime of the sensor system. We develop a mathematical model for the lifetime of the sensor system as a function of system parameters including the “source” and “path” redundancy levels utilized. We discover that there exists optimal “source” and “path” redundancy under which the lifetime of the system is maximized while satisfying application QoS requirements. Numerical data are presented and validated through extensive simulation, with physical interpretations given, to demonstrate the feasibility of our algorithm design.

Lightweight methods are designed by A. Gupta et el., (2006) to detect anomaly intrusions in wireless sensor networks (WSNs). The main idea is to reuse the already available system information that is generated at various layers of a network stack. To the best of our knowledge, this is the first such approach for anomaly intrusion detection in WSNs.

Preventive mechanisms is designed A.P.R da Silva (2005) can be applied to protect WSNs against some types of attacks. However, there are some attacks for which there is no known prevention method. For these cases, it is necessary to use some mechanism of intrusion detection. Besides preventing the intruder from causing damages to the network, the intrusion detection system (IDS) can acquire information related to the attack techniques, helping in the development of prevention systems. In this work we propose an IDS that fits the demands and restrictions of WSNs. Simulation results reveal that the proposed IDS is efficient and accurate in detecting different kinds of simulated attacks.

Many sensor network routing protocols have been proposed method is designed by D. Wagner et al., (2003), but none of them have been designed with security as a goal. We propose security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks-sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. We describe crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.

Trust-based geographic routing approaches is developed by F. Bao et al., (2012) the ideal performance level achievable by flooding-based routing in message delivery ratio and message delay without incurring substantial message overhead. For trust-based intrusion detection, we discover that there exists an optimal trust threshold for minimizing false positives and false negatives. Furthermore, trust-based intrusion detection outperforms traditional anomaly-based intrusion detection approaches in both the detection probability and the false positive probability.

III. SYSTEM MODEL

Trust Based Neighbor Weighted Voting Scheme to strengthen intrusion detection in WSN is evaluate the dynamic radio range of neighbor nodes. Identification of multisource multipath routing for intrusion tolerance at higher levels. Neighbor Weighted Voting algorithm provides trust weight of each neighbor sensor node. Weight threshold is evaluated for marking the sensor node as normal node and malicious node. Discard the communication of internal malicious node by identifying lower weight votes of corresponding sensor node.

The best number of voters and the intrusion invocation interval used for intrusion detection under which the lifetime of a WSN is maximized in the presence of selective capture which turns nodes into malicious nodes capable of performing packet dropping attacks and bad-mouthing attacks.

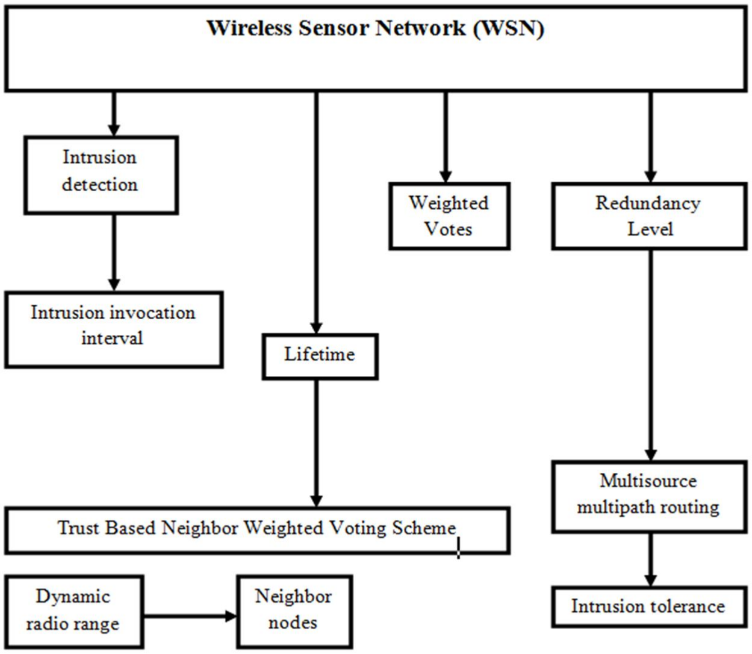
Wireless Sensor Network (WSN)
Intrusion detection
Intrusion invocation interval
Lifetime
Weighted Votes
Redundancy Level
Multisource multipath routing
Intrusion tolerance
Trust Based Neighbor Weighted Voting Scheme
Dynamic radio range
Neighbor nodes

Fig. 1. Architecture Diagram of Trust Based Neighbor Weighted Voting Scheme for Intrusion Tolerance in WSN.

A. Wireless Sensor Network

WSN comprises sensors of different capabilities types of sensors are Cluster Heads (CHs) and Sensor Nodes (SNs). CHs are superior to SNs in energy and computational resources, denote the initial energy levels of CHs and SNs, and applied to any shape of the operational area.

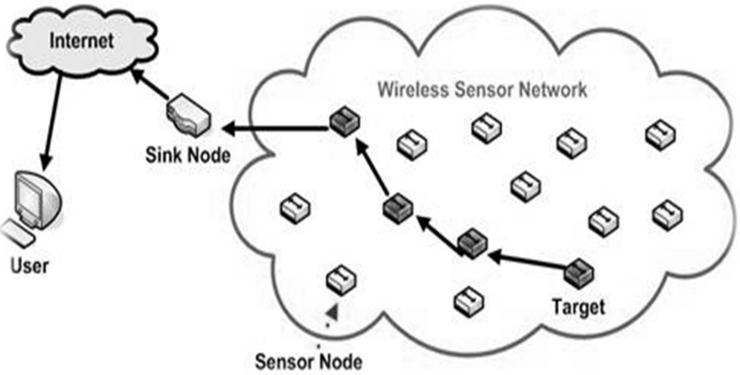

Fig. 2. Architecture of Wireless Sensor Network.

CHs and SNs are distributed in the operational area ensure coverage by deploying CHs and SNs randomly and distributed according to homogeneous spatial Poisson processes. Radio ranges of CH and SN for transmission are initialized. Radio range and transmission power of both CHs and SNs are dynamically adjusted throughout system lifetime to maintain connectivity between CHs and between SNs.

Multi-hop Routing is required for communication between two nodes with distance greater than single hop. Due to limited energy, a packet is sent hop by hop without using acknowledgment or retransmission. All sensors are subject to capture attacks (inside attackers). Since all sensors are randomly located in operational area capture rate applies to both CHs and SNs in turn compromised nodes are also randomly distributed in operation area.

Compromised node performs two most energy conserving attacks, bad-mouthing attacks, packet dropping attacks. Environment conditions cause a node to fail with certain probability include hardware failure and transmission failure (due to noise and interference). Hostility to HWSN is characterized by as per node capture rate, determined based on historical data and knowledge about the target application environment.

B. Query Success Probability and Intrusion Detection Level

Define total number of queries system answer correctly until it fails as lifetime or the mean time to failure (MTTF) of the system translated into actual system lifetime span given the query arrival rate. Failure occurs when no response is received before query deadline due to energy exhaustion, packet dropping by malicious nodes, channel/node failure and insufficient transmission speed to meet the timeliness requirement. Find both optimal redundancy levels and IDS a setting under MTTF is maximized given a set of parameters characterizing operational and environment conditions.

Develop probability model to estimate MTTF of a WSN using multipath data forwarding to answer queries issued from mobile user roaming in WSN area. MTTF formulation first deduce the maximum number of queries system can possible handle before running into energy exhaustion for the best case in which all queries are processed successfully. System evolves dynamically amount of energy spent per query also varies dynamically. Given the query arrival rate λq as input average interval between query arrivals is 1/λq. Estimate amount of energy spent due to query processing and intrusion detection for query based on query arrival time.

C. Dynamic Redundancy Management of Multipath Routing

Dynamic redundancy management dynamically identifies and applies best redundancy level in terms of path redundancy (mp) and source redundancy (ms) and best intrusion detection settings in terms of number of voters (m), intrusion invocation interval (TIDS). Maximize MTTF in response to environment changes to input parameters.

Dynamic redundancy management of multipath routing is distributed in nature describe the CH and SN execution protocols for managing multipath routing for intrusion tolerance to maximize system lifetime. Specify control actions taken by individual SNs and CHs in response to dynamically changing environments. All nodes in the system act periodically to a timer event to adjust the optimal parameter setting in response to changing environments. Optimal design settings are determined at static design time, pre-stored in table over perceivable ranges of input parameter values. As there is no base station in the system, duty of performing table lookup operation with interpolation and/or extrapolation techniques applied to determine optimal design parameter settings assumed by CHs.

D. Neighbor Node Radio Range

Random deployment of sensor nodes (SN) in HWSN distributed according to homogeneous spatial Poisson processes with density. Initial total number of SNs in the system are noted Countermeasure against selective capture of dynamic radio range adjustment with random deployment.

Initial radio range of sensor maintains neighbor connectivity SN adjusts its radio range dynamically throughout its lifetime, to maintain connectivity such that average number of 1-hop neighbor SNs remains. SNs closer to the BS increase radio range more than SNs away from BS to counter selective capture. Any communication between two nodes with a distance greater than single hop radio range between them requires a multi-hop.

E. Trust Based Neighbor Weighted Voting

Trust based Neighbor weighted voting against intrusion to detect and evict compromised nodes. Every SN runs a simple host IDS to assess its neighbors. Host IDS is light-weight to conserve energy, does not rely on the feedback mechanism tied in with a specific routing protocol based on local monitoring each node monitors its neighbor nodes only. Each node uses a set of anomaly detection rules such as high discrepancy in the sensor reading, packet is not forwarded as requested interval, retransmission, repetition, and delay rules. If the count exceeds a system-defined threshold neighbor node that is being monitored is considered compromised.

When the majority of voters come to conclusion that a target node is bad then target node is evicted. System-level false positive probability voters can incorrectly identify a good node as a bad node. System-level false negative probability voters can incorrectly misidentify a bad node as a good node. Derive two system-level IDS probabilities based on bad-mouthing attacks performed by inside attackers.

F. Intrusion Tolerant Optimal Multipath Routing

Intrusion tolerant optimal multipath routing is countermeasure against selective capture of sensor nodes. Achieved through two forms of redundancy source redundancy by which SNs sensing a physical phenomenon in same feature zone are used to forward sensing data to BS path redundancy by which paths are used to relay packets from source SN to the BS. Optimality is achieved by operating SNs in power saving mode, SN is either active (transmitting or receiving) or in sleep mode. For transmission and reception energy consumption of sensors adopt optimal energy model.

BS has pair wise keys with the SNs. SN has a pair wise key with each of its neighbors up to a few hops away for future expandability. SN encrypts data for confidentiality and authentication.

IV. PERFORMANCE RESULTS AND DISCUSSION

To identify the best protocol setting of our countermeasures against selective capture. This includes the radio range to be adjusted dynamically by individual SNs, the best redundancy level used for multipath routing, as well as the best redundancy level in terms of the number of voters and the best intrusion invocation interval used for intrusion detection to maximize the WSN lifetime in the presence of selective capture which turns critical nodes into malicious nodes capable of performing packet dropping attacks and badmouthing attacks.

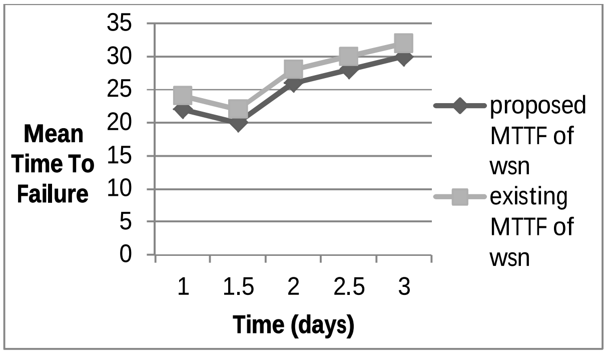

Fig. 3. WSN of Time and Mean Time to Failure (MTTF)

Fig.3 Compares the effect of Time on the MTTF under random capture vs. selective capture at the optimal (*mp*, *ms*) setting under random capture vs. selective capture. We again observe that there exists an optimal value (marked by a black dot) at which the MTTF is maximized. Furthermore, the optimal Time value under selective capture in general is smaller than that under random capture because the system has to increase detection strength to cope with selective capture which creates more compromised critical nodes.

Fig.4 confirms that with the "dynamic radio range adjustment" countermeasure, a SN increases its radio range over time to maintain network connectivity. Further, under selective capture because critical nodes (i.e., when x is small) are more likely compromised, and subsequently detected and evicted from the system, a critical node must increase its radio range more rapidly to maintain network connectivity and improve packet delivery reliability to effectively counter selective capture.

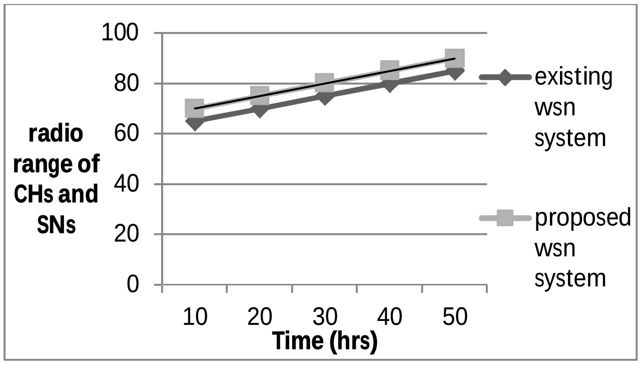

Fig. 4. WSN of Time(hrs) and Radio range of CHs and SN.

V. CONCLUSION

Adaptive network management with three countermeasures for coping with selective captures aiming to create holes near the base station in a wireless sensor network to block data delivery. Through numerical analysis, we demonstrated that our countermeasures are effective against selective capture. There exist best protocol settings in terms of the best radio adjustment, the best redundancy level for multipath routing, the best number of voters, and the best intrusion invocation interval used for intrusion detection to maximize the system lifetime. Leveraging the analysis techniques proposed in this paper, one can obtain optimal protocol settings at static time, store them in a table, and apply a simple table lookup operation at runtime to determine optimal settings for adaptive network management to maximize the system lifetime without runtime complexity.

REFERENCES

[1]Hamid Al-Hamadi and Ing-Ray Chen (2013) ‘Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks’ Vol 10.

[2] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," J. High Speed Netw., vol. 15, no. 1, pp. 33-51, 2006.

[3] G. Bravos and A. G. Kanatas, "Energy consumption and trade-offs on wireless sensor networks," 16th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications, pp. 1279-1283, 2005.

[4] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," 1st ACM Workshop on Quality of Service & Security in Wireless and Mobile Networks, Montreal, Quebec, Canada, 2005.

[5] I.R. Chen, F. Bao, M. Chang, and J.H. Cho, "Trust management for encounter-based routing in delay tolerant networks" IEEE Globecom 2010, Miami, FL, Dec. 2010.

[6] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660-670, 2002.

[7] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," IEEE Int. Workshop on Sensor Network Protocols and Applications, pp. 113-127, 2003.

[8] Y. Lan, L. Lei, and G. Fuxiang, "A multipath secure routing protocol based on malicious node detection," Control and Decision Conference, pp. 4323-4328, 2009.