BANDWIDTH PARAMETER EVALUATION OF PROTOCOLS BOUNDED BY DISTANCEANDSECURELY VERIFIEDIN PROXIMITY OF TWO-HOP NEIGHBOURS

Toby Mathews[1], Malathi P[2]

[1]*Student, Department of E&TC, D.Y.Patil College of Engineering, Akurdi, Maharashtra, India*
[2]*Professor, Department of E&TC, D.Y.Patil College of Engineering, Akurdi, Maharashtra, India*

Abstract

Wireless Sensor Networks (WSN) implemented across a large campus can provide advanced levels of monitoring and control, and authenticated access, over the complete dynamic environment. Access to these WSNs should be controlled and proper authentication schemes designed to prevent unauthorized access. Where access route to a device is not directly available, the authentication scheme must perform effectively over multiple hops. With Distance bounding (DB) protocols, the physical proximity of 2 or more parties is detected and verified. Modification of these protocols allows for extension of the verification to multi hop neighbours. This paper evaluates the performance of the network when routing is done using common wireless protocols and the nodes are under attack. This approach will allow for increased accuracy, while having minimal or no impact on the other transmission parameters.

Keywords: *Wireless Sensor Networks, WSN, Distance Bounding Algorithm, Authentication Accuracy, Packet Delivery Ratio, OLSR)*

----------***----------

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are popular sources to gather data from multifunctional microelectronic devices interacting at short distances to communicate data to collectors. It is possible to conduct WSN deployment, comprising of very small sensor nodes, involving sensing, data processing, and communication parts, which enhances traditional wired sensor networks. This paper investigates the performance of the network; focusing on aggregation of data, routing protocols, wormhole attacks and node authentication. Wireless Ad-hoc data networks rely severely on routing info provided by neighboring users. Here, providing secure, dependable and effective tele-communication procedures for collection of data is vital. Routing decisions of nodes are governed and influenced by the neighbouring nodes, based on multiple parameters like distance, power to live, neighbor list etc. Hence, it is a critical need to authenticate the above neighbours. There are multiple ways of authenticating the neighbours, and Secure neighbour discovery (SND) methods are commonly used. Distance-bounding (DB) protocols, is one of the significant SND methodologies that defines the physical distance, as a limiting factor, between two nodes. Provision of cryptographic proof of the neighbour's proximity can be provided in addition to the validation of the closeness measurement between the nodes, lying beyond the next-hop neighbouring node. The different parameters defining the secure network need to be planned for, and must authenticate parameters such as transmitted data, inter-node distance, as well as the node status claims. (i.e. authenticate the node or not).

A significant parameter for design of the network is the Bandwidth that will need to be factored in for the data transmission. The extra overheads for the security implementation could strain the existing power demands on nodes.

1.1 Background

Existing Studies

Most of the studies conducted have focused on the basics of the Network protocols, in a limited challenge environment.

In this paper, traditional DB protocols in a 2 hop setting are stretched to a new concept for utilizing and extending the DB protocols over two-hop and more neighbours. This ensures distant nodes are not spoofed by external parties to appear as neighbours, and prevents two-hop routes to distant nodes being advertised by malicious valid and/or compromised. Analysis of the different bandwidth parameters under these specific conditions are evaluated. This leads to the derivation of proof for the impact inference. This paper also discusses the effectiveness of this protocol under the effect of dishonest actions by the untrusted immediate, also called as next hop nodes, and the two-hop neighboring nodes, also known as provers.

[2] This paper proposed a node authentication protocol for WSNs, and show how its implementation can be combined inside distinct routing protocols. There are 2 benefits to the integration among routing and authentication. One, authentication is ruled by routing; where only those nodes

on a data communication route to the base station validate each other. Unnecessary protocol executions are hence rejected. Two, compromised and malicious nodes are unable to use utilize routing protocols to inject themselves into data routes. A flat WSN is assumed, i.e., no clustering or cluster heads. Node mobility problems are addressed by proposing an authentication protocol that an initially authenticated node uses when its position changes. Therefore, nodes attempt to learn common keys at the same time that they try to discover routing paths. A node executes the protocol with another node guided by the need to direct (or relay) data but not with all its neighbors, and therefore energy is saved. Finally, when nodes are mobile, routing paths and the key graph need to be updated and, occur as a single integrated step.

Simulations using software environments or actual nodes need to be carried out in order to evaluate the performance of the protocol in practical conditions

[3] The focus of this paper was on the protocol flexibility against deceptive nodes within the network that disrupt communications. Earlier studies have presented that, routing protocols are made increasingly resilient by the additionof randomness and methods of data duplication. The enemy cannot predict routes due to the diversification provided. A new framework, theoretical in nature is proposed, highly based on random walks that are influenced, and occur on a torus lattice. The resilience of the protocols is increased, to survive against insider attacks, using random walk theory with a bias introduced, applied in the environment focussed on security. As conventional unbiased walks in random nature are unfitting due to the extended routes, the main aim, is conducting an impact analysis, to evaluate random walk bias, while being attacked by insiders.

The energy outflow levels reached while successfully transmitting a packet increases exponentially, in cases where unbiased random walk designs are utilized. Packets can reach the destination faster aided by the bias introduced, hence providing better rates of delivery and saving energy. The diversity of the routes reduces along with the high bias values. Schemes to detect anomalies can be designed to deliver configurable and strong rhythms to reduce power in the non-presence of attacks.

[4] This paper focused on different distance bounding protocols suitable for the RFID technology. Regrettably, these are typically designed using an informal style, which leads to imprecise studies and biased comparisons. The authors propose an enhanced analytical design of the distance bounding protocols using a combined framework. This framework includes a detailed study of vocabulary related to frauds, adversary, and prover. It inspects the capabilities, assets and strategies of the adversaries in the network, and addresses the influence of the prover's ability to interfere with his device. New ideas in the distance bounding area are introduced viz. the black-box white-box models, and the relationship between the frauds impacting these models. The relevancy and result of the framework is authenticated on a case study: Munilla-Peinado distance bounding protocol.

In this paper, distance bounding protocols are analyzed using a methodical method. The fair assessments provided by this framework can be used to design or analyze distance bounding protocols.

[5] Protocols used for Distance bounding (DB) permit one unit, usually the node acting as a verifier, to securely get a limit on the upper distance bound to the prover. DB, in the papers before this, was measured mostly in a single verifier and prover environment. Group settings in Secure DB have not had much research conducted prior to this paper. Group settings are defined as a network design including a set of provers and verifiers interacting amongst themselves in an environment. Group distance bounding (GDB) protocols are motivated by practical applications and circumstances, i.e. pairing devices in groups, and admission governors based on location. This research debates, one-directional protocols for GDB utilizing a new primitive for passive DB and explains methodology for passive DB protocol and its usage to produce a secure and efficient Group DB protocol for several uni-directional GDB situations.

A DB could be created by a passive verifier, without having knowledge of the position of (or distance to) a verifier node in active mode. Other non-critical data about distances to other nodes, might allow Passive DB to acquire joint GDB protocols These protocols, in group settings, can be impacted by denial-of-service attacks

[6] The network protocols related to, and being used now by WSNs have been mainly intended for effective energy utilization. In this paper astudy was directed into the security procedures and processes planned for individual network layers (application, network and data-link layers). This paper, reviews currently available data, and examines the security vulnerabilities related to routing, info-aggregation, and user verification in WSN situations. The conclusion by this paper are that presently accessible security services are improperly designed and executed, thereby exposing WSNs towards several attack types. This data should not be changeable, holds its integrity and remains private.

Restricted power sources and computational skills of sensor networked nodes pushes collection technologies to concentrate on battery efficiency, factoring that some information will be conceded and trusting exclusively on the probability that missing information is non-contiguous or usable. A driven attacker will crack any existing WSN, and therefore the conclusion that these networks are inappropriate for applications where data security is highly critical. e.g. military use.

1.2 Problem Statement

Improve the bandwidth utilization of the network when in cryptographic based authentication solution for wireless sensor nodes in 2 hop scenarios in the Distance Bounding

phase, where routing is done using OLSR and its variants and the nodes are facing Wormhole attacks.

Implement routing protocol in the WSN model, analyze detection and prevention of Wormhole attacks, implement cryptography based authentication solution scheme.

To analyze performance of WSN on basis of the following Network parameters - Packet delivery ratio, Throughput, End to end delay.

Plot the impact of these parameters under the specified conditions.

2. METHODOLOGY

The overall nodes are randomly distributed in an area that is under observation. A node is marked as a source and another as Destination. The communication or transfer of data is to happen between these nodes. In line with the needs of WSNs under study under the paper being studied, there is sufficient distance and nodes between the source and destination.

A simulation is created to show transmission between the source and destination when the nodes are static or stationary with respect to each other and when they are mobile. Very fast mobility is not a case under study here i.e. nodes do not move faster than the handshake or authentication happens between them. The nodes help authenticate the next hop before moving out of range of the existing path. The WSN uses OLSR to define a path between these mobile nodes.

With the path that is created the nodes act as independent nodes to be able to receive transmissions or even initiate transmissions themselves.

All the nodes are assumed to have constant power at the beginning. The simulation tries to calculate the utilization of the available limited energy while under these conditions.

The WSN is measured under the following parameters –

1. When the nodes are under ideal conditions – no attacks, all authenticated nodes, source and destination reachable by a defined path.
2. When a specific node is under Wormhole attack – authenticated nodes, source and destination reachable by a defined path
3. When the nodes in the path are invalid

Under all these conditions the WSN setup is measured for specific changes on Bandwidth related parameters such as Packet delivery ratio, End to End delay, overall throughput, of the nodes.

The base paper is proved in the sense of authentication still being valid even though nodes in the path are invalid and/or under attack. Instead of a probabilistic study of the nodes and their pass through authentication, this project has proved that the practical implementation of these concepts is fairly economic and achievable under simulated conditions.

The authentication used is a mix of the different flavours of OLSR. Since the overall target is to measure the performance of the environment in an attack scenario, the actual protocols provide very less contribution to the effect on the measured parameters. Under a condition of all attacks, the WSN network performs well under the simulated conditions to be able to be used in practical real world situations. The default multi hop scenario has an inbuilt a time limit for authentication handshake. The round trip delay measured can help with ensuring there is a second level of protection against the hacking into of nodes.

In cases of contactless cards, where a spy node can be introduced between the card and reader to try and capture the card information is a good example of this application. The authentication protocol shows that the overall end to end authentication holds strong even under multiple iterations and larger data chunks. Similarly, there would be a larger power consumption in case of Invalid nodes in the network. This is a parameter than can be measured to alert to suspicious activity on the network.

Access control to different locations in a campus. If the card reader is under a wormhole attack, there will be different ways of detecting it. Also the overall performance of the network will deteriorate in terms of data being transmitted and received. In module 1, a simple transmission channel is designed that has 15 wireless nodes, Rayleigh propagation, uses OLSR routing protocol. Source is considered from Node 0 and Destination Node 14. Constant Bit Rate (CBR) traffic model is utilized. The simulation demonstrates the working of OLSR protocol even when the nodes are moved around. With the nodes advertising their positions, newer more efficient paths are designed.

To expand upon this design, we include the Distance bounding protocol into the Wireless design. The code measures the distance using a time bound, and transfers encrypted data between two nodes separated by another one. This is the essence of the Distance bounding protocol.

Two wormhole attack nodes are introduced to test the efficacy of the Distance bounding protocols along with the standard authentication used by the OLSR routing. The data being transmitted is encrypted using AES and decrypted at the receiving node. The wormhole attack scenario is shown in the below snapshot of the simulation. With the definition of individual models, it is seen that successful transmission of data packets is achieved between nodes in a simulated environment. The transmission and reception of the data between the Source and Destination is simulated in 3 different configurations.

Direct transmission - Here the nodes are defined to be to straight linked to each other. The defined path between source and destination ensures the transmission is directed with minimum interference.

Valid user - In this scenario, the path between source and destination contains 2 valid nodes that are validated to be secure. The transmission uses this as secure route and the parameters are measured.

Invalid user - With the introduction of invalidated nodes, the path between source and destination has to be created by the routing protocol being used. The encryption and authentication protocols ensure data being transmitted is not lost.

3. CONCLUSION

The parameters focused on Bandwidth utilization, measured for the simulations conducted are plotted below.

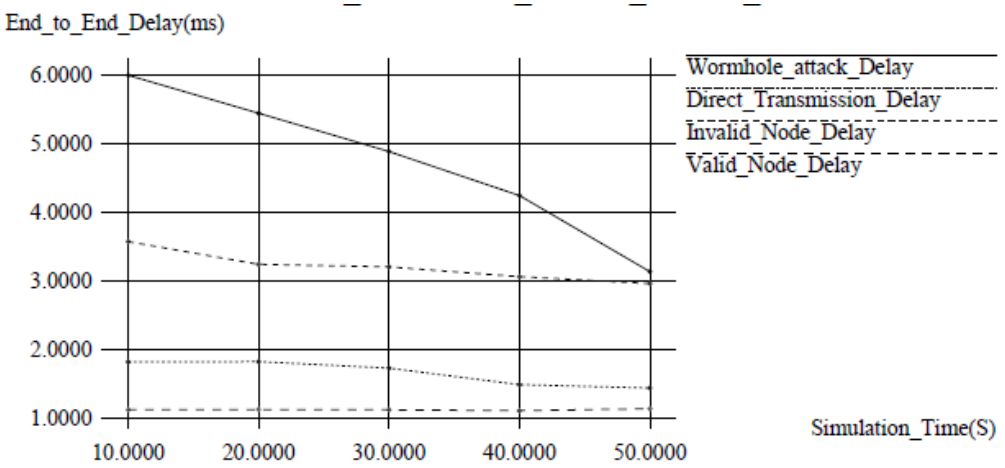

Fig -1: End to End delay

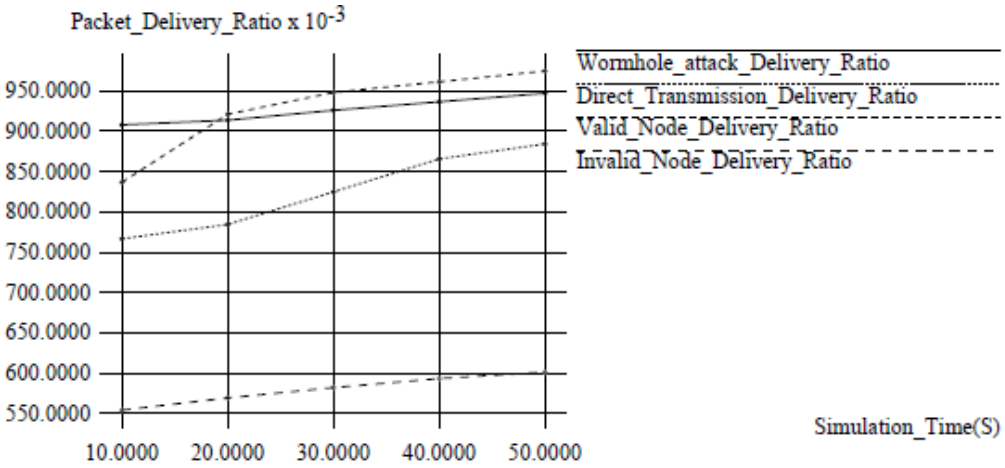

Fig -2: Packet Delivery Ratio

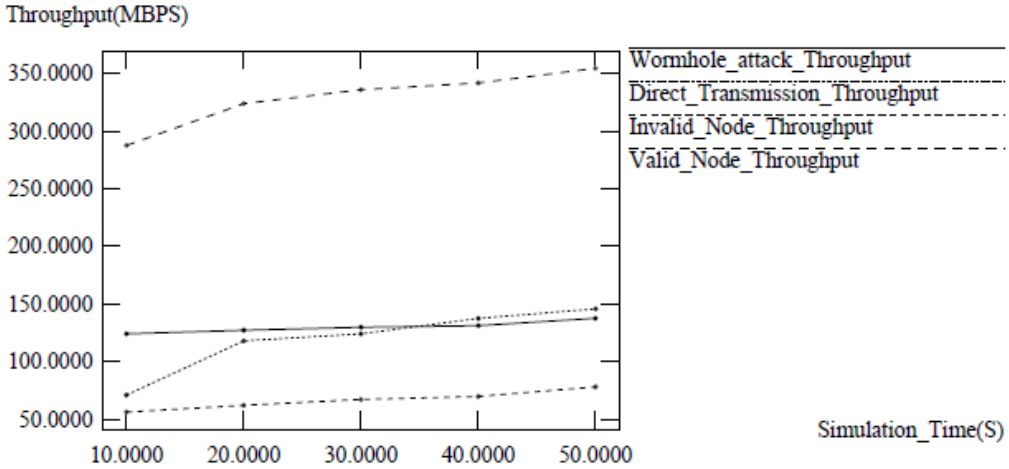

Fig -3: Throughput

The results show that the bandwidth utilization has a direct correlation with the attacks on the nodes. The transmission of data has to be repeated multiple times to be effective. The presence of invalid nodes and nodes under a wormhole attack, lead to larger delays and lower Packet delivery ratio.

REFERENCES

[1] Elena Pagnin, Gerhard Hancke, and AikateriniMitrokotsa, "Using Distance-Bounding Protocols to Securely Verify the Proximity of Two-Hop Neighbours" IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 7, JULY 2015

[2] Amandeep Kaur and Sukhwinder Singh Sran, "Detection of packet – dropping attack in recoverable concealed data aggregation protocol for homogeneous wireless sensor networks", "2015 Fifth International Conference on Advanced Computing & Communication Technologies, 2015 IEEE DOI 10.1109/ACCT.2015.102"

[3] Sandeep Kumar, S.M. Kusuma, B.P. Vijaya Kumar, "Random Key distribution based Artificial Immune System for Security in Clustered Wireless Sensor Networks", 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science

[4] Binod Kumar Mishra, Mohan C. Nikam, Prashant Lakkadwala, "Security Against Black Hole Attack In Wireless Sensor Network–A Review""2014 Fourth International Conference on Communication Systems and Network Technologies, 978-1-4799-3070-8/14"

[5] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless adhoc networks" IEEE Communications Magazine, 40(10):70–75, 2002

[6] Muazzam A. Khan, Ghalib A. Shah, Muhammad Sher, "Challenges for Security in Wireless sensor Networks (WSNs)," World Academy of Science, Engineering and Technology 56 2011.

[7] R. Kompella, J. Yates, A. Greenberg, and A. Snoeren. "Detection and localization of network black holes", In Proceedings of IEEE INFOCOM, pages 2180–2188, 2007

[8] E. Ngai, J. Liu, and M. Lyu. "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks". Computer Communications, pages 2353–2364, 2007

[9] Alexander Betts, Frank Meyer-Bodemann, Fred Muller and Shao Ying Zhu "Wireless Sensor Network Security: A Critical Literature Review", "978-1-4673-5756-2/13/$31.00 ©2013 IEEE. From the 2013 IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems (COMCAS 2013), Tel Aviv, Israel, 21-23 October 2013"

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Sensor Network Protocols and Applications, 2003" Proceedings of the First IEEE. 2003 IEEE International Workshop on, pp. 113-127, 2003.Reference 1

BIOGRAPHIES

Toby Mathews is a Student in the E&TC Department, D.Y. Patil College of Engineering, Pune. He received Bachelor of Engineering degree in 2003 from University of Mumbai, India.

Dr. Mrs. P. Malathi is a highly awarded Professor in the E&TC Department, D.Y. Patil College of Engineering, Pune. She has over 22 years of teaching and postgraduate guiding experience. Her focus field is Wireless Communication among other technologies