Middle-East Journal of Scientific Research 24 (11): 3554-3559, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.3554.3559

A Trustworthy and Reliability Model for Reconfigurable Wireless Sensor Networks

[1]Vaddi Naga Padma Prasuna, [2]A. Valarmathi, [3]J. Arputha Vijaya Selvi and [2]P. Senthil Pandian

[1]Dept of ECE, Atria Institute of Technology, Bangalore, India
[2]Dept. of Computer Applications, Anna University-BIT Campus, Tiruchirappalli, India
[3]Dept of ECE, Kings College of Engineering, Pudukkottai, India

Abstract: The use of Wireless Sensor Networks (WSNs) has become an incredible part of every field of communication applications. WSNs operate under challenging conditions such as energy, memory and processing limitations. These resource constraints adversely impacts trust and reliability of the WSN. Reconfigurable WSN Architecture (RWSN) has been introduced and discussed elsewhere along with its advantages. Trust and reliability of WSN is an active research topic and various models and approaches were proposed by researchers. In this paper a Trust and Reputation model adaption in to RWSN discussed and its evaluation results using TRMSim-WSN presented.

Key words: TRUST · Trust and Reputation Systems · Reconfigurable Wireless Sensor Networks · TRMSim · Wireless Sensor Network (WSN)

INTRODUCTION

Trust and Reputation in WSN, TRM Models: Trust in a Reconfigurable Wireless Sensor Networks is a probability at which actions will occur. Reputation [1, 3] has been defined as anticipation of a node's behavior based on current and past transactions.

Trust Reputation Models are a forward-looking solvent for computation of trust in a Wireless Sensor Network (WSN) and also provides security for the applications designed based on WSN proposed RWSN architecture

Trust Reputation Models - Review

Reputation-Based Framework for Sensor Networks (RFSN): Ganeriwal and Srivastava [6] proposed RFSN. In this model each sensor node maintains the reputation for neighbor node. Trust value is evaluated on the basis of that reputation and they use Bayesian formulation for representing reputation of a node. It considers that each node maintains good relationship with neighbor nodes to reach stationary state. The drawback of this model is it lacks of stability under high mobility conditions. In RFSN, no node is allowed to disseminate bad reputation information, also sometimes faces uncertain problems

Parameterized and Localized Trust Management Scheme (PLUS): Yao *et al*. [7] proposed Parameterized and Localized trust management Scheme (PLUS) for security of a WSN. This model is based on localized distributed approach and trust is calculated based on either direct or indirect observations. They introduced a routing scheme named PLUS_R has been adapted for their PLUS scheme. The drawback of this system is that the authors assume that all the important control packets generated by the BS must contain a Hashed Sequence Number (HSN). Inclusion of HSN in control packets not only increases the size of packets resulting in higher consumption of transmission and reception power but also increases the computational cost at the SNs. It keeps the record of a parameter database to describe the operational environments, application types and network status and node information.

Agent-Based Trust And Reputation Management (ATRM): Boukerche *et al*. [8] have proposed an ATRM scheme for WSNs. This scheme is based on a clustered WSN with mobile agent and calculates trust in a fully distributed manner. It works on specific agent-based platform. It assumes that there is a single trusted authority, which is responsible for generating and launching mobile agents, which makes it vulnerable against a single point of failure.

Corresponding Author: Vaddi Naga Padma Prasuna, Dept of ECE, Atria Institute of Technology, Bangalore, India.
E-mail: prasuna.edu@gmail.com.

Group-Based Trust Management Scheme (GTMS): Group-based Trust Management Scheme (GTMS) [9] used in clustered WSNs. The significance of GTMS is it evaluates the trust values of individual nodes, which requires less memory for storing the data base of trust values. It uses two topologies namely intragroup topology considers distributed trust management approach and intergroup topology uses centralized trust management approach is followed. This approach helps to reduce the cost of trust evaluation of distant nodes. GTMS helps in finding malicious nodes, independent of specific routing scheme.

Heuristic Approach based Trust Worthy Architecture (HATWA): V. R. Sarma Dhulipala *et al*.[10] have proposed HATWA for sensor network that considers the challenges of the system and focus on the collaborative mechanism for trust evaluation and maintenance. It is capable of fulfilling critical security, reliability, mobility and performance requirements for reliable communication while being readily adaptable to different applications. HATWA architecture involves three heuristic algorithms such as security, mobility and reliability which involve the functioning of network monitoring node architecture. These models are introduced to redesign the issues and challenges in the trust management for WSN.

Reconfigurable Trustworthy Architecture (RTWA): The data communication transactions in the RWSN can be obtained based on the trustworthiness or reputation factor. The concept of Trust Reputation System (TRS) can be applied to our proposed model RWSNA [2,11] which are considered as RTWA for the evaluation of the trust. The overall trust value of a WSN comprises of direct and indirect trust values [3] and the same approach applicable for RWSN. As trust varies dynamically [4,11] so considering it as a decimal number whose value ranges from -1 to +1. If the communication or any event or any transaction has to take place between the two nodes then the Reconfigurable network monitoring node [2] evaluates the trustworthiness of the node in our proposed model.

The advantage of our proposed model is it can be deployed in any field i.e. biology, military, cultivation etc. According to the applications there is need to change only the internal logic of RMP (Reconfigurable Management Plane) the rest of the block functionalities remains same. Cost of the deployment, time to update will be reduced by adopting the Reconfigurability. The block diagram of Reconfigurable Network monitoring node architecture of RTWA is shown in Fig.1.

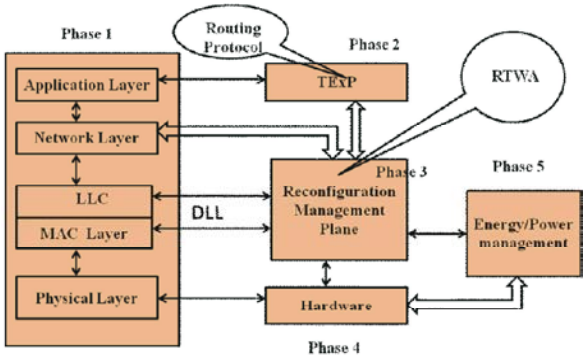

Fig. 1: Reconfigurable Wireless Sensor Network Monitoring Node architecture

RMP Controller: This RMP plays a key role in our proposed framework. RMP controls the stack of all the layers for exchange of control signal with each other. These layers are characterized with the ability to undergo reconfigurability of their firmware components and architectures which enhances the flexibility in dynamic conditions.

Physical Layer: RMP control the physical layer when it needs to be undergone reconfiguration process for servicing high end devices with high mobility or dynamic topology.

Network Layer: RMP outperforms on network layer for topology control when this layer adapts the Reconfigurability of networking services like to facilitate address/IP changing, network topologies, network firmware and parameters, protocols in a dynamic network.

MAC: RMP controls scheduling at MAC layer, It also controls the access protocols of the MAC layer for a dynamic changing network topology.

TExP Protocol: It is used as a routing protocol between the application layers RMP. The trust values of sensor nodes can be collected/ communicated by this protocol to RMP controller.

Working Principle: Reconfigurable network monitoring node controls the dynamic topology of a WSN [2] by considering trust factor of the nodes. Thus it further enhancement of trustworthiness of the system as a whole for reliable communication. As stated the overall trust of a RWSN is the contribution of individual trusts i.e. RWSN security, RWSN mobility, RWSN reliability, RWSN communication model. RNMN working model consists of multiple phases.

Phase 1: It is stack of different layers considered as protocol stack plays a prominent role to build the overall trust in the phase 1 module.
Phase 2: It is used for secure routing considered TExP protocol [5].
Phase 3: The Reconfigurable management plane acts as a main controller
Phase 4: controlling of energy power management in RTWA.
Phase 5: Energy management by adapting to DPM (Dynamic and power management techniques)

Evaluation of Trust of a Node in RWSN: Algorithm

Initial Condition: Exchange of data with neighboring nodes,
$R_f V$=0.2 (is a probabilistic value, varies from 0 to 1)
Input value: Authenticated Node ID, RSM, RMM, RRM, RCM of the nodes.

Begin:
Initial trust value of a node in RWSN = $T_{int} = (ST + UT)/T_t$
where $T_{t=} (ST + UT)$;
If ($T_{int} > R_f V$)
Data is allowed to communicate with neighboring/ targeted nodes.
else consider the trust of the Reconfigurable security model of a node.
T_{RS}=ED + SRD + SP;
If ($T_{RS} > R_f V$)
Exchange of data or communication with the targeted node
else evaluate the Reconfigurable trust in mobility model of a node.
If node is stationary or constant
Then consider trust mobile value in a RWSN =0
Else evaluate the Reconfigurable Trust value of a node in dynamic state
T_{RM} = HD+ OE+D;
if ($T_{RM} > R_f V$)
data communication is allowed
else consider the Reconfigurable trust of reliable model
T_{rrel} = DA + $E_{DA;}$
if ($T_{Rrel} > R_f V$)
then allow for data exchange
else evaluate the overall Reconfigurable trust value in communication model
T_{RCM} = E_{TRF} + CMP;
If ($T_{RCM} > R_f V$)
data communication is allowed;
else evaluate the overall of a node in a RWSN.
OVT = T_{int} + T_{RS} + T_{RM} + T_{Rrel} + $T_{RCM;}$
if (OVRT > $R_f V$)
data communication is allowed.
else
Communication with neighbor nodes is not permitted.

End.

Notations:
ST: Successful transactions
UT: Unsuccessful transactions
T_t: Total transactions
Tint= Initial Trust evaluation value
$R_f V$= Reference value of the trust
$T_{RM =}$ Reconfigurable mobility model trust value
$T_{Rrel =}$ Reconfigurable reliable model trust value
T_{RS} = Reconfigurable Security model trust value
$T_{RCM=}$ Reconfigurable Communication model trust value
ED= Encrypted data
SRD = Secure routing of data
SP = Secure protocol
OE_M = optimized Energy consumption in mobility
HD= Hopping distance from the source
D= Delay incurred
DA = Data aggregation
ED_A = Energy consumption during data aggregation
E_{TRF} = Energy consumption for tranceiving functionalites.
OVRT = overall Reconfigurable trust value

RTWA - Evaluation Results and Analysis: The trust values of a RWSN are simulated using TRMSim. It is a simulator to analyze and compare trust and reputation models. This simulator also supports to visualize the number of idle nodes, the benevolent nodes, malicious nodes, client nodes and relay nodes.Nodes support switching over to idle state, as well as oscillating their behavior and acting in collusion with other malicious sensors [1].

Simulation Environment: The simulation is performed using TRMSim-WSN 0.5 version [5]. Considered a RWSN whose parameters are considered listed in table 1 [1]. Created network topologies can be loaded from saved XML files. The nodes are dynamic in a grid fashion, considered free space wireless channel, IEEE 802.11 MAC protocol and TExP routing protocol [6].The main significance of TExP routing protocol is for trust value exchange between the authenticated node ids. The simulation of the network has been performed by considering the parameters listed in the Table 1.

Table 1: Sensor Network Specifications

S.No	Parameters	Considered Values
1	Clients	15 %
2	Relay Servers	5 %
3	Radio range	12
4	Min No of nodes	50
5	Max No of Nodes	50
6	No of networks	5
7	Number of executions	5
8	Trust and Reputation model	BTRM_WSN
9	Terrain dimension	1000 m x 1000 m2
10	Simulation time	750 ms
11	Routing protocol	TExP
12	No of clusters	5
13	Initial battery of each sensor node	1x 106 J
14	Power Consumption for transmission	1.6 W
15	Power Consumption for reception	1.2 W
16	Power Consumption in idle state	1.15 W

The Fig. 2 represents the WSN before the simulation and Fig.3 represents after simulation of the network where in which nodes move dynamically.

Accuracy: The WSN metric accuracy is used for the representation of reliability and security level [7, 8] of our proposed model. The accuracy is shown in percentage which is the representation selection of trustworthy nodes within a total number of transactions.

Path Length: It signifies about the average hops contributing by clients towards the most trustworthy sensors in a chosen TRM model. It is considered that the lower the average path length the better the trustworthiness is as it will free from security attacks, less delay and less energy consumption. (Data exchange) Transactions speed can be enhanced as server nodes are nearer to the clients.

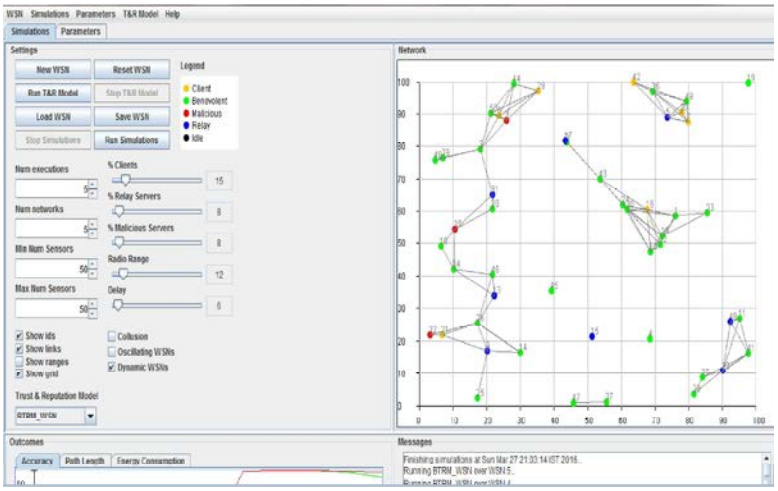

Fig. 2: Topology of a network before simulation

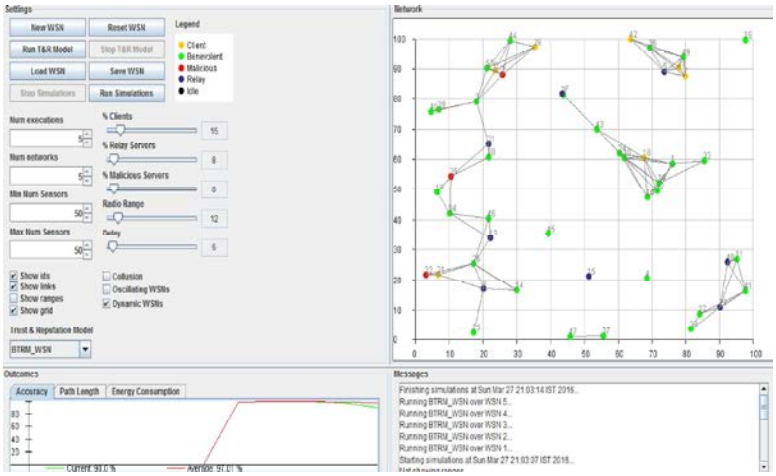

Fig. 3: Topology of a network after simulation

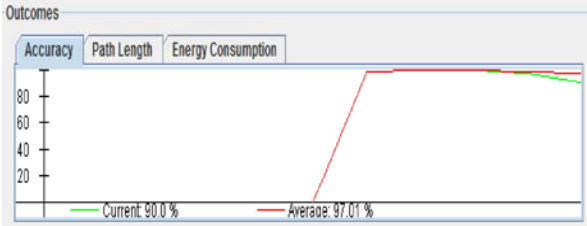

Fig. 4: Representing accuracy

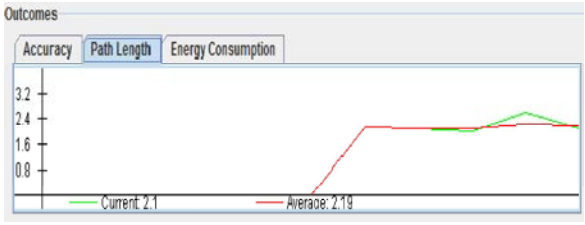

Fig. 5: Representing Path Length

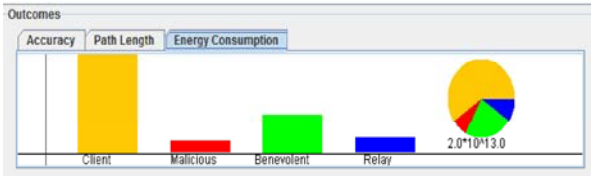

Fig. 6: Representing messages of the output window

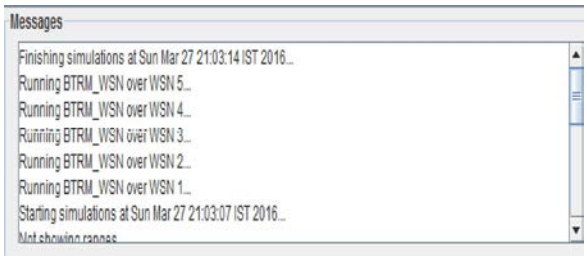

Fig. 7: Representing messages of the output window

Energy Consumption: It signifies about the overall energy consumption of a network i.e.:- is energy consumption of a client nodes for request sending messages, energy consumption of malicious nodes for processing unwanted services, Energy consumption by server nodes for sending the responses, energy consumption by relay nodes, energy consumed for processing and finding the trustworthy nodes based on considered TRM model.

CONCLUSION

Various research approaches about adaption of trust and reputation model in WSN has been discussed. We discussed about our Reconfigurable Wireless Sensor network monitoring node and its working principle considering trust and reputation factors. The trust and reliability computation works as a function of a reconfigurable hardware by using Reconfigurable management plane in conjunction with the TRM modules can greatly enhance the efficiency and flexibility of WSNs in the topology control when the nodes are in dynamic nature. Implementation and evaluation of Trust and Reputation model using TRMSim simulator and the evaluation results has been presented.

REFERENCES

1. Marzi, H. and M. Li, 2013. An Enhanced bio-inspired trust and reputation model for wireless sensor network. Procedia Computer Science, 19: 1159-1166.
2. Prasuna, V.N.P., A. Valarmathi and J.A.V. Selvi, 2016. Finite state Markovian model for trustworthy reliable communication in dynamic Reconfigurable Wireless Sensor Network architecture. In Emerging Trends in Engineering, Technology and Science (ICETETS), International Conference on (pp: 1-6). IEEE.
3. Karthik, N. and V.S. Dhulipala, 2011. Trust calculation in wireless sensor networks. In Electronics Computer Technology (ICECT), 2011 3rd International Conference on (4:. 376-380). IEEE.
4. Liu, Zhaoyu, Anthony W. Joy and Robert Thompson, 2004. A dynamic trust model for mobile ad hoc networks. Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of. IEEE,
5. Mármol, F.G. and G.M. Pérez. 2009. TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. Communications, 2009. ICC '09. IEEE International Conference on. Dresden: IEEE, 2009. 1-5.
6. Ganeriwal, S. and M.B. Srivastava, 2004. Reputation-Based Framework for High Integrity Sensor Networks. In Proceedings of ACM workshop security of ad hoc and sensor networks (SASN '04), pp: 66-67.
7. Yao, Z., D. Kim and Y. Doh, 2006. PLUS: Parameterized and localized trust management scheme for sensor networks security. In Proceedings of third IEEE international conference on mobile ad-hoc and sensor systems (MASS '06), pp: 437-446.
8. Boukerche, A., X. Li and K. EL-Khatib, 2007. Trust-based security for wireless ad hoc and sensor networks. Computer Communications, 30: 2413-2427.

9. Shaikh, R.A., H. Jameel, B.J. d'Auriol, H. Lee, S. Lee and Y.J. Song, 2009. Group-based trust management scheme for clustered wireless sensor networks. Parallel and Distributed Systems, IEEE Transactions on, 20(11): 1698-1712.
10. Dhulipala, V.S., N. Karthik and R.M. Chandrasekaran, 2013. A novel heuristic approach based trust worthy architecture for wireless sensor networks. Wireless personal communications, 70(1): 189-205.
11. Prasuna, V.N.P., A. Valarmathi and J.A.V. Selvi, 2016. Parametric analysis of a novel Reconfigurable Wireless Sensor Network architecture. In Emerging Trends in Engineering, Technology and Science (ICETETS), International Conference on (pp: 1-5). IEEE