Journal of Engineering and Applied Sciences 14 (12): 4191-4199, 2019
ISSN: 1816-949X

Dirichlet Distribution Based Trust Model for Malicious Node Detection in Wireless Sensor Network

[1]V. Uma Rani and [2]K. Soma Sundaram
[1]Department of Computer Science and Engineering, Jaya Engineering College,
Bharathiar University, Tamil Nadu, Chennai, India
[2]Aarupadai Veedu Institute of Technology, Department of Computer Science and Engineering,
Tamil Nadu, Chennai, India

Abstract: In recent days, misbehaving node or malicious node detection in Wireless Sensor Networks (WSN) becomes essential, due to its distributed nature and its increasing demand in various applications. Malicious attacks damages communication between sensor nodes causing the loss of packets, reduced forwarding behaviour of nodes and creating insecure data transmission. Trust model is one of the solutions to provide security in WSN but most of the trust models are susceptible to bad mouthing and ballot attack. In this study, we propose a Dirichlet Distribution based Model (DDTM) to detect malicious attacks, like black hole attack, selective forwarding attack and on/off attack. DDTM uses trinomial Dirichlet distribution for trust evaluation of sensor nodes. DDTM uses Dirichlet fusion rule to combine the opinions gathered from neighbouring nodes and standard deviation rule to overcome bad mouthing and the ballot attack of the trust models. Further, in our proposed DDTM, we include a penalty scheme and a dynamic sliding window scheme to find attacks quickly and provide malicious behaviour feedback to the routing model for secure data transmission. The results of proposed DDTM shows an increased ability compared to present trust models to detect node based attacks and an increase in packet delivery ratio of wireless sensor networks.

Key words: Trust, Dirichlet distribution, malicious node, wireless sensor network, sliding window, sensor nodes

INTRODUCTION

With the rapid development of distributed applications and wireless communication technology, Wireless Sensor Networks (WSN) has widely applied to several applications like industrial monitoring applications, security surveillance and medical applications, so on. WSN consists of large tiny sensors with various sensing capabilities to monitoring hostile or unattended environment (Jin *et al*., 2018). However, due to its open wireless medium, WSN faces various threats from inside and outside of its network. Several cryptography techniques have developed to prevent outsider threats (Puneeth *et al*., 2018) but insider threats are not easy to detect, since, they compromise nodes and have access to the network by revealing valid cryptography keys (Rani and Sundaram, 2014). Such compromised node disrupts communication between sensor nodes and decreases the overall network performance. Some examples of the most dangerous insider threats are black hole attack, selective forwarding attack and on/off attack. In black hole attack, the compromised node falsely notifies other nodes that is nearer to sink and drops all the packets routed to it. The selective forwarder selectively drops sensitive packets. The on/off attack causes malicious node forward packets in specific time.

Existing solutions applicable for wireless networks to detecting insider threats are not suitable for WSN due to its restricted power, reliability and scalability factors (Kharb and Sharma, 2016). Without any solutions like trust model (Shamshirband *et al*., 2014) for malicious attacks, WSN suffers from exploitation and fails to provide adequate services as a network. Trust model provides a soft security solution by establishing cooperative behaviour among nodes to improve secure communication among them. Trust model (Rehman *et al*., 2017) can be applied to give secure information during cluster head selection (Yan *et al*., 2010), data aggregation (Kumar and Dutta, 2016) and routing (Bao *et al*., 2011).

Trust models provides subjective (Han *et al*., 2014) opinion based on direct trust or indirect trust. Direct trust evaluated from direct observations and indirect trust evaluated from indirect observations of sensors. Direct

Corresponding Author: V. Uma Rani, Department of Computer Science and Engineering, Jaya Engineering College,
Bharathiar University, Tamil Nadu, Chennai, India

trust specifies opinion about any given sensor node by evaluating its behaviour directly. The indirect trust specifies opinion about any given sensor node by acquiring beliefs filtered from its neighbour nodes (Chen *et al*., 2011). The trust models combine direct trust and indirect trust to found the overall trust of sensor nodes and hence are capable of detecting failure and malicious activity in a sensor node by analyzing its behaviours (Anisi and Analoui, 2011).

However, trust model itself suffers from reputation based attacks (Momani *et al*., 2014) like badmouthing and ballot attack. In bad mouthing attack, a malicious node gives negative feedback about neighbour sensor nodes to decrease the trust rating of those sensor nodes. In ballot attack, a malicious node gives positive feedback to increase trust ratings about malicious sensor nodes.

In this study, a Dirichlet distribution based trust model has proposed to detect malicious node based attacks in WSN. DDTM also has resilient mechanism to safeguarding it from bad mouthing and ballot attack.

Literature review: This study provides a concise review of existing trust models to detect malicious misbehaviours and their shortcomings in WSN.

In study Anita *et al*. (2013) have developed a two-way acknowledgment-based trust framework for wireless sensor networks (2-ACKT). It calculates direct trust based on link layer acknowledgment scheme. The 2-ACKT scheme counts the number of packets forwarded and dropped during data transmission during interval "t" for direct trust calculation. The trust evaluation in the 2-ACKT scheme is poor and it fails to respond on/off attacks, selective forwarding attacks with low probability ratio and a reputation based attacks. The researcher (Shaikh *et al*., 2009) have developed a Group based Trust Management Scheme (GTMS) for wireless sensor network. GTMS uses dynamic timing window to measure the successful and unsuccessful interactions. It evaluates the direct trust from data collected from updating timing window periodically. It resists selfish, malicious and faulty nodes but is unable to detect on/off attack with low probability ratio. Since, good and bad behaviour of a malicious node maintains their reputation ratings does not fall below to trust threshold.

Liu *et al*. (2016) have developed an active-trust based routing protocol for preventing the black hole attack in the homogeneous wireless sensor network. The active trust scheme effectively reduces malicious node by detecting alternative trusted route between sources to destination. The active trust scheme has no mechanism for detecting on/off attack and selective forwarding attack. Ye *et al*. (2017) have developed a Dynamic Trust Evaluation Model (DTEM) for monitoring the behaviour of sensor nodes. It calculates direct trust value by weighted based evaluation scheme. It uses a sliding time window mechanism for monitoring node at regular intervals. It adjusts the value of the weights for integrating direct trust and indirect trust based on interactions between nodes. It is suitable for detecting a black hole attack, on/off attack and selective forwarding attack. But it has no prevention mechanism for reputation based attacks.

Haibo *et al*. (2018) have proposed a trust evaluation method for efficient node utilization in wireless sensor network. It uses information entropy to detect malicious misbehaviour in wireless sensor network. It provides quick convergence to detect malicious attacks but it cannot resist reputation based attacks. Zhang *et al*. (2014) built a ML-TRUST mechanism to analyze the misbehaviours and to enable the trusted cooperation among nodes. It collects recommendation from n-hop neighbours also about different possible routes like single, parallel and overlapping routes. It avoids false recommendations using fraud rule and consistent factors. Ren *et al*. (2016) have proposed a Channel Aware Reputation System (CRS-A) for detecting selective forwarding attack in wireless sensor networks. It uses the beta distribution of trust evaluation of neighbours. CRS-A scheme avoids the malicious node being selected as next hop during routing.

Yang *et al*. (2017) have proposed an incomplete beta distribution to optimize the trust model to enhance the security of sensors. Cho and Qu (2013) have proposed a source level trust evaluation technique to detect selective forwarding attack. It detects packet droppers by using the beta and entropy trust model. Wang and Liu (2017) proposed a node based behaviour monitoring which uses Bayesian filter based on beta distribution to detect faulty nodes. Beta distribution based trust model provides the binomial opinion for checking the node trustworthiness. Ponomarchuk and Seo (2010) have developed a trust model based on traffic monitoring system. It uses exponential distribution and threshold based scheme to detect the anomaly behaviour of sensor nodes. Ghosal and Halder (2014) have developed a Gaussian distribution based trust model for detecting intruders in the distributed wireless sensor network. Gaussian and exponential distribution based approaches have used to handle situations when outcomes are continuous random variables.

Several computational trust models using probability distribution to detect malicious misbehaviour in WSN. They use beta distribution, exponential distribution, Uniform or Gaussian distribution and Dirichlet distribution

of trust evaluation. These trust models differ mainly in how they define and compute new reputation based on existing behaviour of sensors. But most of the trust models suffers to detect all kinds of packet forwarding misbehaviour like on/off attack and selective forwarding attack with low probability ratio and some of them was unable to protect itself reputation based attacks. So, we have developed a DDTM Model to efficiently detect node based malicious misbehaviours like black hole attack, on/off attack and selective forwarding attack with varying probability ratio. It also overcomes the reputation based attacks such as ballot attack and bad mouthing attack.

MATERIALS AND METHODS

Dirichlet distribution based trust model

Structure of Dirichlet distribution based trust model: The Dirichlet distribution based trust model is an unsupervised, localized mechanism that relies on every sensor node. It does not need any training and adapts to dynamic environments easily. DDTM establishes the trust relationship between sensor nodes and selecting sensor nodes with a high degree of trust for any given routing. This model has two modules, namely monitoring module and trust evaluation module. Monitoring module observes the activities of sensor nodes and gives direct observation and indirect observation to the trust evaluation module. The trust evaluation module calculates a trust of the sensor nodes and classifies the sensor nodes based on trust value. It gives information to the routing module for trusted communication. Figure 1 shows the structure of Dirichlet distribution based trust model. Table 1 shows the various notations used in DDTM.

Monitoring module: The DDTM uses monitoring module for observing the activities of sensor nodes in 1-hop away. It is important for the trust model to calculate direct trust of sensor nodes. It has three data structures such as Store vector, S, F and P-count. The Store vector stores all packets sent by sensor nodes. The S-count specifies the number of packets forwarded during communication. The F-count specifies the number of packets dropped. F-count is number of packets remains in the Store vector. P-count specifies the number of packets modified during specific interval. The monitoring module observes the behaviours of sensor nodes and updates these counts during the specified data transmission time. Initially, the sensor node calculates the Data Transmission time (DTR) for neighbour sensors and checks whether neighbour sensor forward packets within a data transmission time. The Data Transmission time (DTR) is the measure of time taken by sensor node to send packets. The monitor module passes this observed information to trust evaluation model for trust evaluation.

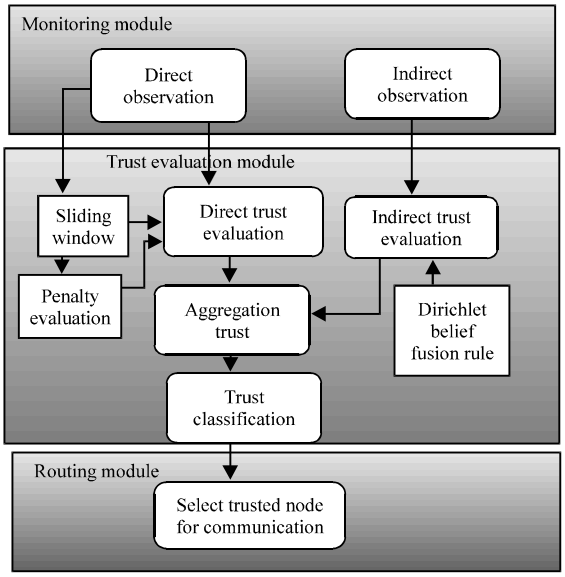

Fig. 1: Struture of DDTM Model

Table 1: Notations used in DDTM

Notations	Meaning
$\vec{p}$	Probability distribution vector
$\vec{x}$	Observation vector
p_1, p_2	Probability values of observed parameters
CT_j^i	Current trust value of node j by node i
DTR	Data Transmission time
RT_j^i	Reputation value of node j by node i
PF_j^i	Penalty factor of node j by node i
., .1, .2	Time factor
S-count, x_1	Number of packets forwarded
i, j, A, B	Sensor node
F-count, x_2	Number of packets dropped
x_3	Uncertainty count
n_j	Uncertainty count factor
IDT_j^i	Indirect trust value from i about j
r_j^A, r_j^B	Reputation value of j
$_j^{AB}$	Standard deviation of reputation
OT_j^i	Overall trust value of j
T_{min}	Minimum threshold for OT

Trust evaluation module: DDTM evaluates the trust using a direct trust evaluation and indirect trust evaluation. It uses the Dirichlet distribution for current trust evaluation. The Dirichlet distribution (Josang, 2007) is a generalized beta distribution that handles multiple discrete random variables. It is sound and flexible model for trust evaluation. DDTM updates trust based on current trust and reputation information stored in a sliding window. The sliding window store recent information by updating observation periodically. DDTM calculates penalty factor by counting the uncertainty value appeared within an observed interval. The penalty factor reduces the trust value of malicious nodes. DDTM evaluates indirect trust by collecting information from neighbors. It gives quicker convergence to trust aggregation. DDTM

aggregates direct trust and indirect trust to produce overall trust value. DDTM classifies a neighbor sensor nodes based on overall trust value.

Direct trust evaluation: DDTM collects observations from the monitoring module for direct trust evaluation. It uses Dirichlet distribution for direct trust evaluation. Dirichlet distribution is a multinomial probability distribution of set of vectors and its probability density function returns the belief of neighbor sensors. We use Dirichlet distribution $\text{Dirichlet}(\vec{p}\,|\,\vec{x})$ expressed using the gamma function as:

$$\text{Dirichlet}(\vec{p}\,|\,\vec{x}) = \frac{\Gamma(x)}{\prod_{i=1}^{k}\Gamma(x_i)}\prod_{i=1}^{k} p_i^{x_i-1} \quad (1)$$

The probability expectation value of Dirichlet distribution is:

$$E\left(\text{Dirichlet}(\vec{p}\,|\,\vec{x})\right) = \frac{x_i}{x_0} \text{ where } x_0 = \sum_{i=1}^{k} x_i \quad (2)$$

Here, $\vec{p}$ is a probability distribution vector represents set of possible outcomes such as:

$$\vec{p} = \{p_1, p_2, p_3\}$$

Where:

p. = The probability of forwarding packets
p. = The probability of dropped packets
p. = The probability of modified packets

Let $\vec{x}$ denotes set of positive real numbers such that $\vec{x} = \{x_1, x_2, x_3\}$ and it denotes vector of observation count of the possible outcomes. The parameter x. represents the number of packets forwarded, x. represents the number of packets dropped and x. represents the number of modified packets.

By using Eq. 2, the current trust of node 'j' calculated from node 'i' is given by:

$$CT_j^i = \frac{x_1+1}{x_1+x_2+x_3+3} \quad (3)$$

In order to give more weight to recent observations over older ones, the current trust CT: and the stored reputation value RT: reevaluates the direct trust DT: by Eq. 4. TDDM uses time factor and penalty factor in trust evaluation for quick detection of malicious behavior:

$$DT_j^i = \alpha RT_j^i + (1-\alpha)CT_j^i - PF_j^i \quad (4)$$

Here, PF: is the penalty factor, « is the time factor. It ranges from 0...1 and « can be chosen based on RT: and CT:. If current trust value is greater than the reputation value and then « is set to «. otherwise, it is set to «. It ranges from 0-1. The update of penalty factor is:

$$PF_j^i = \frac{n_j}{x_0+3} \quad (5)$$

Here, n. is the uncertainty count factor. DDTM calculates n. from the sliding window. The penalty factor PF: decreases the trust value of malicious node and detects consecutive misbehavior of node quickly.

Sliding window scheme: The DDTM uses the dynamic sliding window to store all previous behaviours of sensor node reputation value which give additional support to calculate the trust value. It improves adaptability, save node memory and enhances the accuracy of trust quantification. The size of sliding window size varies dynamically based on the packet dropping behaviour of sensor nodes. It set the uncertainty value u. by Eq. 6:

$$u_j = \begin{cases} 1 & \text{if PDR}>0.2 \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

Based on packet dropping ratio, DDTM increases one time unit of window size. It counts the number of uncertainty (u.) occur within a window and uses this count to calculates penalty value of that sensor node which is specified in Eq. 5. The sliding window size can be increased up to the largest size for each uncertainty arises within a window. If uncertainty reduces, then the size of the window reduces to smallest size of the sliding window. The size variation of sliding window easily predicts the behaviour of sensor nodes.

Indirect trust evaluation: Indirect trust module collects trust information r. from the neighbor sensor nodes. It uses the standard deviation rule to find the deviation among opinions gathered from neighbors. Let A and B be a two neighbours which gives opinion about j. DDTM evaluates the standard deviation of opinion by Eq. 7:

$$\sigma_j^{AB} = \sqrt{\frac{r_j A_{r_j} B}{\left(r_j^A + r_j^B\right)^2\left(r_j^A + r_j^B + 1\right)}} \quad (7)$$

The variations of opinions are smaller then it can be fused together by the Dirichlet belief fusion rule. The Dirichlet belief fusion rule is defined by Eq. 8:

$$IDT_j^{A\circ B} = r_j^A \times \gamma^A + r_j^B \times \gamma^B \quad (8)$$

Aggregation of trust and trust classification: Each sensor node i evaluate trust of j by evaluating the total trust which is given by:

$$OT_j^i = \frac{DT_j^i + IDT_j^i}{2} \quad (9)$$

Based on overall trust value, DDTM classifies nodes as three sets, namely good set, suspicious set and bad set based on the trust value. The node is in a bad set if trust value is in the range [0-0.5], a suspicious set if trust value is in the range [0.5-0.7] and a good set if trust value is in the range [0.7-1]. During communication, each sensor node selects the next hop based on its distance and trust information. The routing module of sensor node collects reputations of one hop neighbours from DDTM Model and select trusted neighbour for communication. If trusted neighbour is not available, then it propagates information back to the downstream neighbours to choose an alternate route. If trusted neighbour is found, then this process continues for all upstream neighbours until it reaches the sink.

RESULTS AND DISCUSSION

In order to test DDTM with sliding window and without sliding window and existing 2-ACKT and GTMS performance, we use network simulation software and take simulation area 500×500 m with 100 nodes deployed randomly with transmission ranges was 50 m. We use IEEE 802.15.4 MAC protocol evaluates both proposed and existing trust model performance under varying attack probability ratio. Table 2 shows the simulation parameters used in DDTM.

The result of DDTM evaluates the sensor node behaviour by detecting a black hole attack, selective forwarding attack and on-off attack. Table 3 shows the parameters for monitoring neighbour sensor nodes and its trust evaluation.

The result shows the reputation evaluation under sliding window size varies from 1-10. The DDTM calculates the uncertainty count from the sliding window by checking the sensor forwarding behaviour exceed uncertainty threshold. DDTM evaluates penalty factor based on uncertainty count rises within a window. The sliding window size varies based on the uncertainty count within a window. Every uncertainty factor increases the window size up to 10. For each observation period, direct trust evaluation based on the historical information within a sliding window and new observation interval. DDTM calculates observation interval based on the neighbour data transmission time. The observation time is greater than the neighbour timeout and then decreases its value otherwise double it. DDTM evaluates the overall reputation and categorize neighbour node as good set, suspicious and bad set.

Table 2: Simulation parameters

Parameters	Values
Simulation time	300 sec
Simulation area	500×500 m
Number of nodes	100
Node deployment	Random
Traffic source	CBR
Number of malicious nodes	Maximum 25
Transmission range	50 m
Propagation model	Free space
Movement of node	Static

Table 3: Trust parameters

Parameters	Values
Trust threshold	0.5
Search packet time	10 sec
Store packet time	15 sec
Neighbour timeout	10 sec
Observation time	10 sec
Number of behaviours measured in each unit	20
Number of units in sliding window	1-10

Trust value evaluation during attacks: The trust value calculation is important for the trust model to quickly detect and recover from attacks. In this study, discuss how the trust value is evaluated by DDTM, DDTM without window, 2-ACKT and GTMS trust models for varying attack probability ratio of malicious nodes.

Trust value evaluation during black hole attack: The black hole attack causes the malicious sensor node to drop all packets pass through them. The continuous misbehaviour of malicious node causes the decrements of reputation value continuously. Figure 2 shows the reputation value analysis of malicious node in DDTM, DDTM without window, 2-ACKT and GTMS trust models. It shows GTMS and DDTM has similar behaviour due to sliding window scheme. DDTM converge quickly to other trust models due to both penalty scheme and sliding window scheme.

Trust value evaluation during on/off attack: DDTM analyses the on/off attacker misbehaviour by creating attacker in two different ways by frequent off period 50% off time and 50% on time for regular forwarding time) and less off period (25% off time and 75% on time for regular forwarding time).

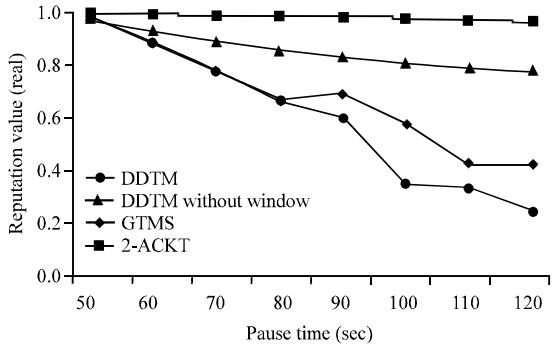

Fig. 2: Reputation value analysis of a node during black hole attack

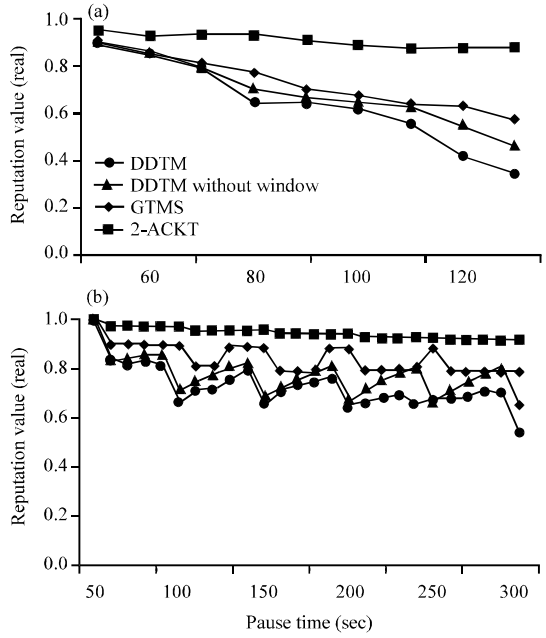

Fig. 3: Reputation value analysis of a node during on/off attack: a) On time-50% and off time-50% and b) On time-75 % and off time-25%

If an off period is takes more than 50% off time then the node misbehaviour was easily detected but it is hard to detect less off period. But the use of sliding window and penalty factor, DDTM responds well for on/off attacks with varying probability value. Figure 3a, b shows the reputation value of the node during on/off attacker.

Trust value evaluation during selective forwarding attack: Selective forwarding attack causes packet drops on certain packets without forwarding all packets to sink. If packet dropping ratio of selective forwarders is very less then attack is difficult to detect it. DDTM analyses

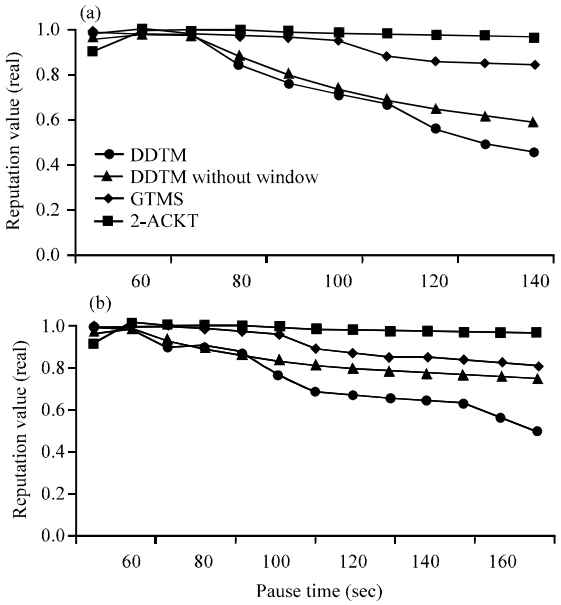

Fig. 4: Reputation value analysis of a node during selective forwarding attack: a) Data forwarding rate -50% and b) Data forwarding rate -80%

the malicious behaviour of selective forwarders by a different compromising probability ratio of forwarding behaviour.

Figure 4a, b shows how DDTM responds well for selective forwarders with a forwarding rate (50 and 80%) during the evaluation period. It shows DDTM responds well for different packet forwarding rate of selective forwarders.

From this reputation analysis, maximum number of rounds needed for attack detection in DDTM, DDTM without window (DDTM-WW), GTMS and 2-ACKT with varying attack probability ratio.

Badmouthing and ballot attack analysis: The DDTM trust model uses direct trust evaluation method to avoid bad opinions from neighbour nodes. If direct trust information is not available, then it uses indirect trust information for reputation evaluation. It avoids bad opinions by calculating the standard deviation among trust values collected from sensors. The neighbour sensor nodes with similar deviations are acceptable and cumulative fusion rule combines the opinion, respectively. DDTM rejects opinions with larger deviations and it avoids wrong opinions in reputation evaluation (Table 4).

Table 5 illustrates the standard deviations of opinions for bad mouthing and ballot attack analysis. Here the node 1 collects the opinion about node 3-6 from neighbour nodes A and B. The standard deviation of opinion about node 4 is high. So, DDTM ignores this

Table 4: Number of rounds for attack detection

Attack models	DDTM	DDTM-WW	GTMS	2-ACKT
Black hole attack	5	7	6	24
Selective forwarding attack -80%	5	6	5	34
Selective forwarding attack -50%	6	11	7	57
Selective forwarding attack -20%	11	47	ND	ND
On/Off attack -50%	5	7	7	92
On/Off attack -25%	18	27	ND	ND

*ND- Not Detected

Table 5: Standard deviation of reputation analysis of node

Node 1	r_i^A	r_i^B	σ_i^{AB}
3	0.95	0.90	0.0942
4	0.90	0.50	20.1700
5	0.96	0.95	0.0859
6	0.81	0.74	0.0977

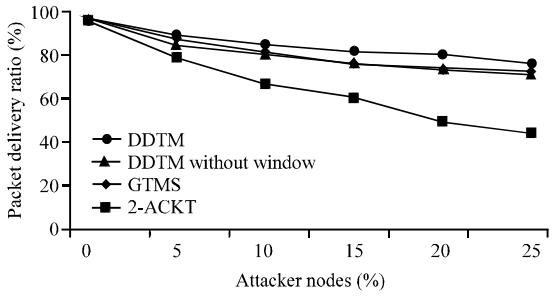

Fig. 5: Paket delivery ratio analysis with varying attacker nodes

observation and it collects opinions from other neighbours. In this way TDDM Model avoids bad opinions for trust calculation.

Performance analysis: DDTM performance was evaluated by the following metrics: packet delivery ratio, energy consumption, end to end delay and storage overhead. Packet delivery ratio specifies the ratio of total packets received to total number of packets sent. Energy consumption specifies average energy consumed by each node during simulation. End to end delay specifies a delay of packets from source to sink and storage overhead specifies the amount of storage additionally needed for reputation evaluation.

Packet delivery ratio analysis: The malicious node drops all packets or drops certain packets or drops at specific time, respectively, reducing the number of packets reaching destination. The trust model of DDTM, GTMS and 2-ACKT identify the malicious nodes and isolate them from 1 the network. Figure 5 shows the packet delivery ratio of trust models under different attack ratio's. As a result, the packet delivery ratio of DDTM, GTMS and 2-ACKT increased based on quick detection of a malicious node in the WSN. The DDTM increases the packet delivery ratio compared to other trust models because of is quicker detection and isolation of malicious node.

Table 6: Storage overhead analysis

Trust models	Storage overhead
RFSN	33 (n-1)
PLUS	32.375 (n-1)+28
ATRM	38 (n-1)
GTMS	44 (n-1)

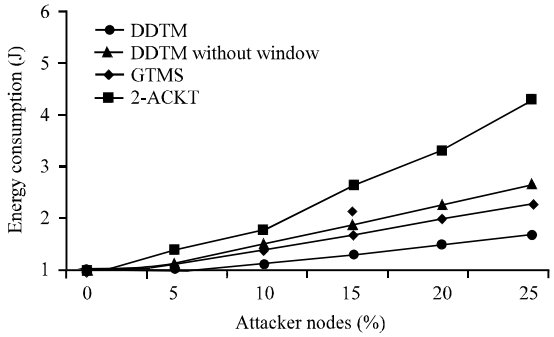

Fig. 6: Energy consumption analysis

Energy consumption and end-to-end delay analysis: Energy consumption is important for wireless sensor networks since it specifies the lifetime of sensor networks. The following Fig. 6 shows the energy consumption analysis for DDTM, DDTM without window, GTMS and 2-ACKT.

The end to end delay specifies the amount of time taken from the sensor node to sink for data. The malicious node increases the end-to-end delay of packets but quicker detection decreases the overall delay during transmission. Figure 7 shows the end-to-end delay analysis for DDTM, DDTM without window and GTMS and 2-ACKT.

Storage overhead analysis: The DDTM requires extra overhead for their storage which are in an acceptable range. Each sensor node maintains a reputation table to store reputation values, so, it requires storage overhead for storing the reputation value which is 16×|n-1| or 8×|n-1| where n-1 is the number of neighbour nodes. The storage needed for storing the reputation value is 16-8 bits based on real or integer form. So, DDTM provides storage overhead compared to other trust models discussed in (Shaikh *et al*., 2009) is shown in Table 6.

A simulation result shows the DDTM Model can effectively resist attacks like black hole attack, on/off attack, selective forwarding attack and reputation based attacks. It improves efficiency of trust model using sliding window and penalty factor. The DDTM Model evaluates the node behaviour under different attack probability

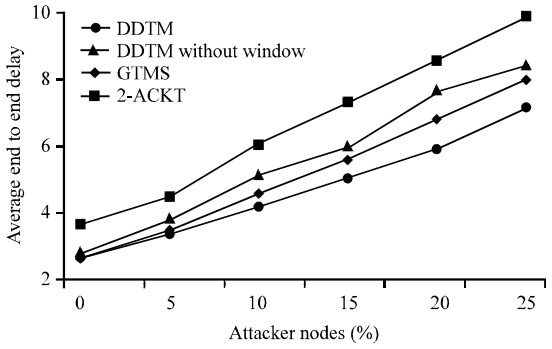

Fig. 7: Average end to end delay analysis

ratio. It takes lesser calculation, effectively increases the packet delivery ratio and decreases the number of packets dropped during transmission. DDTM provides less end to end delay and less energy consumption compared to other trust models. DDTM Model assists the routing process and detects an forwarding attacker quickly.

CONCLUSION

In this study, DDTM has proposed to detect node based forwarding misbehaviors efficiently. It uses forwarding behavior, dropping behavior and packet modification behavior to detect black hole attack, selective forwarding attack and on/off attack. It detects the varying behavior of selective forwarders and on/off attackers by the dynamic sliding window and penalty factor. It also protects nodes from badmouthing attack and ballot attack. The DDTM assists the routing process to enhance communication in wireless sensor networks. Future work can taken up as more parameters like mobility, data reliability in DDTM to assists the aggregation process of hierarchical wireless sensor networks and to detect other kinds of attacks.

REFERENCES

Anisi, M. and M. Analoui, 2011. Multinomial agents trust modeling using entropy of the dirichlet distribution. Intl. J. Artif. Intell. Appl., 2: 1-11.

Anita, X., J.M.L. Manickam and M.A. Bhagyaveni, 2013. Two-way acknowledgment-based trust framework for wireless sensor networks. Intl. J. Distrib. Sens. Netw., 9: 1-14.

Bao, F., I.R. Chen, M. Chang and J.H. Cho, 2011. Hierarchical trust management for wireless sensor networks and its application to trust-based routing. Proceedings of the 2011 ACM International Symposium on Applied Computing, March 21-24, 2011, ACM, New York, USA., ISBN: 978-1-4503-0113-8, pp: 1732-1738.

Chen, D., G. Chang, D. Sun, J. Li, J. Jia and X. Wang, 2011. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. Comput. Sci. Inform. Syst., 8: 1207-1228.

Cho, Y. and G. Qu, 2013. Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs. Intl. J. Distrib. Sens. Netw., 9: 1-16.

Ghosal, A. and S. Halder, 2014. Tailor-made gaussian distribution for intrusion detection in wireless sensor networks. Proceedings of the IEEE 11th International Conference on Ubiquitous Intelligence and Computing and 2014 and IEEE 11th International Conference on Autonomic and Trusted Computing and IEEE 14th International Conference on Scalable Computing and Communications and its Associated Workshops (UTC-ATC-ScalCom), December 9-12, 2014, IEEE, Bali, Indonesia, ISBN:978-1-4799-7646-1, pp: 406-411.

Haibo, S., Z. Kechen and Z. Hong, 2018. A trust evaluation method for improving nodes utilization for wireless sensor networks. KSII. Trans. Internet Inf. Syst., 12: 113-1135.

Han, G., J. Jiang, L. Shu, J. Niu and H.C. Chao, 2014. Management and applications of trust in wireless sensor networks: A survey. J. Comput. Syst. Sci., 80: 602-617.

Jin, M., X. Gu, Y. He and Y. Wang, 2018. Wireless Sensor Networks. In: Conformal Geometry: Computational Algorithms and Engineering Applications, Jin, M., X. Gu, Y. He and Y. Wang (Eds.). Springer, Cham, Switzerland, ISBN: 9783319753324, pp: 253-296.

Josang, A., 2007. Probabilistic logic under uncertainty. Proceedings of the 13th International Australasian Symposium on Theory of Computing (CATS' 07) Vol. 65, January 30- February2, 2007, Australian Computer Society, Inc., Darlinghurst, Australia, pp: 101-110.

Kharb, K. and B. Sharma, 2016. Reliable and congestion control protocols for wireless sensor networks. Intl. J. Eng. Technol. Innovation, 6: 68-78.

Kumar, M. and K. Dutta, 2016. LDAT: LFTM based data aggregation and transmission protocol for wireless sensor networks. J. Trust Manage., 3: 2-20.

Liu, Y., M. Dong, K. Ota and A. Liu, 2016. Active trust: Secure and trustable routing in wireless sensor networks. IEEE. Trans. Inf. Forensic. Secur., 11: 2013-2027.

Momani, M., M. Takruri and R. Al-Hmouz, 2014. Risk assessment algorithm in wireless sensor networks using beta distribution. Intl. J. Comput. Netw. Commun., 6: 157-166.

Ponomarchuk, Y. and D.W. Seo, 2010. Intrusion detection based on traffic analysis in wireless sensor networks. Proceedings of the 2010 19th International Annual Conference on Wireless and Optical Communications (WOCC), May 14-15, 2010, IEEE, Shanghai, China, ISBN:978-1-4244-7597-1, pp: 1-7.

Puneeth, D., N. Joshi, P.K. Atrey and M. Kulkarni, 2018. Energy-efficient and reliable data collection in wireless sensor networks. Turk. J. Electr. Eng. Comput. Sci., 26: 138-149.

Rani, V.U. and K.S. Sundaram, 2014. Review of trust models in wireless sensor networks. Intl. J. Comput. Inf. Syst. Control Eng., 8: 371-377.

Rehman, E., M. Sher, S.H.A. Naqvi, K. Badar Khan and K. Ullah, 2017. Energy efficient secure trust based clustering algorithm for mobile wireless sensor network. J. Comput. Netw. Commun., 2017: 1-8.

Ren, J., Y. Zhang, K. Zhang and X. Shen, 2016. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. IEEE. Trans. Wirel. Commun., 15: 3718-3731.

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. IEEE Trans. Parallel Distrib. Syst., 20: 1698-1712.

Shamshirband, S., N.B. Anuar, M.L.M. Kiah, V.A. Rohani, D. Petkovic, S. Misra and A.N. Khan, 2014. Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. J. Network Comput. Applic., 42: 102-117.

Wang, J. and B. Liu, 2017. Online fault-tolerant dynamic event region detection in sensor networks via trust model. Proceeddings of the 2017 IEEE International Conference on Wireless Communications and Networking (WCNC), March 19-22, 2017, IEEE, San Francisco,California,USA.,ISBN:978-1-5090-4184-8, pp: 1-6.

Yan, L., Y. Pan and J. Zhang, 2010. Trust cluster head election algorithm based on ant colony systems. Proceedings of the 3rd International Joint Conference on Computational Science and Optimization (CSO) Vol. 2, May 28-31, 2010, IEEE, Huangshan, China, ISBN:978-1-4244-6812-6, pp: 419-422.

Yang, Y., X. Jin, S. Yao, X. Qiu and L. Liu, 2017. Reputation detection based on incomplete ß distribution for mobile agent in wireless sensor networks. Intl. J. Distrib. Sens. Netw., 13: 1-13.

Ye, Z., T. Wen, Z. Liu, X. Song and C. Fu, 2017. An efficient dynamic trust evaluation model for wireless sensor networks. J. Sens., 2017: 1-16.

Zhang, B., Z. Huang and Y. Xiang, 2014. A novel multiple-level trust management framework for wireless sensor networks. Comput. Netw., 72: 45-61.