Detection of Selective Forwarding Attacks in Wireless Sensor Networks using Channel-Aware Adaptive Detection Threshold

J. Jayabharathi[1] Dr. R. Saminathan[2] Dr. G. Ramachandran[3]
[1]Research Scholar [2,3]Assistant Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]Annamalai University Annamalainagar – 608 002, Tamil Nadu, India

Abstract— Wireless Sensor Network (WSN) are vulnerable to selective forwarding attacks that can maliciously drop a subset of packets for degrading network performance and endanger the information security. Meanwhile,due unstable to wireless channel in WSN the packet loss rate during the communication of sensor nodes may be high and varying from time to time. In this paper Channel-aware Reputation System with Adaptive Detection Threshold in Wireless Sensor Networks (CADT) to detect selective forwarding attacks is proposed. The CADT evaluates the data forwarding behaviors of the sensor nodes, according to the deviation from monitored packet loss and estimated normal loss. To optimize the detection accuracy of CADT, the optimal threshold for forwarding evaluation is adaptive to time varied channel condition and the estimated attack probabilities of compromised nodes. Furthermore an attack-tolerant data forwarding scheme is developed to collaborate with CADT for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network. Extensive simulation results demonstrate that CADT can accurately detect the selective forwarding attacks and identify the compromised sensor nodes, while the attack-tolerant data forwarding scheme can significantly improve the data delivery ratio of the network.

Key words: CADT, AODV, PREQ, PREP, TCP, UDP, TCL, SAT

I. INTRODUCTION

In Wireless Sensor Networks, packet event monitoring and data gathering technique, has been widely applied to both military and civilian applications. Many WSNs are deployed in unattended and even hostile environments to perform mission-critical tasks, such as battlefield reconnaissance and homeland security monitoring. However, due to the lack of physical protection, sensor nodes are easily compromised by adversaries, making WSN vulnerable to various security threats [1], [2]. One of the most severe threats is selective forwarding attack, where the compromised nodes can maliciously drop a subset of forwarding packets to deteriorate the data delivery ratio of the network. It also has significantly negative impacts to data integrity, especially for data-sensitive applications, e.g., health-care and industry monitoring. On the other hand, since WSNs are generally deployed in open areas (e.g., primeval forest), the unstable wireless channel and medium access collision can cause remarkable normal packet losses. The selective forwarding attacks are concealed by the normal packet losses, complicating the attack detection. Therefore, it is challenging to detect the selective forwarding attacks and improve the network performance. However, for the WSNs deployed in hostile environments where the wireless channel is unstable, normal packet loss rate highly depends on the wireless channel quality that varies spatially and temporally. If we use a measured or estimated normal packet loss rate to detect selective forwarding attacks, some innocent nodes may be falsely identified as attackers due to the time-varied channel condition. For instance, if a mobile obstacle abruptly blocks the data transmission of two sensor nodes, the unexpected packet losses may mislead the attack detection. Therefore, a flexible and fault-tolerant evaluation technique is crucial to accurately identify the attacks and compromised sensor nodes [7], [8]. Meanwhile, due to the negative impacts of selective forwarding attacks, data delivery ratio of a network becomes the primary performance metric for resisting the attacks. Although compromised sensor nodes can be accurately identified, they are still available candidates [9] to forward data for other sensor nodes before physically renewed or replaced. If a compromised node launches attack with a low probability but has good channel condition, it may forward more data packets than a normal node with poor channel condition, in spite of the malicious drops. Therefore, it is of paramount importance to design an attack-tolerant routing scheme to make full use of these nodes or stimulate their cooperation for improving the data delivery ratio. In this work, a Channel-aware reputation System with Adaptive Detection Threshold (CADT) to detect selective forwarding attacks in WSNs is proposed. Specifically, the network lifetime to a sequence of evaluation periods is divided. During each evaluation period, sensor nodes estimate the normal packet loss rates between themselves and their neighboring nodes, and adopt the estimated packet loss rates to evaluate the forwarding behaviors of its downstream neighbors along the data forwarding path. The sensor nodes misbehaving in data forwarding are punished with reduced reputation values by CADT [4]. Once the reputation value of a sensor node is below an alarm value, it would be identified as a compromised node by CADT.

Aim of this research work is,

- To evaluate the forwarding behaviors of sensor nodes by utilizing an adaptive detection threshold.
- To develop a distributed and attack-tolerant data forwarding scheme to collaborate and improve the throughput of the network.
- To achieve a high detection accuracy with both false and missed detection probabilities and improve the data delivery ratio for the network.

A. AD HOC on Demand Distance Vector Protocol (AODV)

AODV is a reactive routing protocol, which does not maintain routes from every node to every other node. Instead, it quickly discovers routes to new destination nodes as and when necessary. The routes are maintained as long as it is necessary. Every mobile node in the network maintains a routing table which stores the next hop node information for a route to the destination node. When a source node

All rights reserved by *www.ijsrd.com*

wishes to route packets to a destination node, it checks the routing table if a fresh enough route is available in the routing table, it makes use of that route. If no route is available in the routing table, then the node discovers a route by broadcasting a *Route Request* (RREQ) message to its neighbors. All the nodes that receive RREQ check its own routing table, if they do not have route to the destination node it increment the hop count and broadcast the RREQ packet to their neighbors and also updates the routing table for a reverse route to source node. When the RREQ query reaches either the destination node itself or any other intermediate node that has a current route to the destination, *Route Reply* (RREP) message is sent back to the source node. The intermediate nodes update the forward route to destination as the RREP propagates to the source node. This RREP is a unicast message.

II. LITERATURE SURVEY

The basic idea from existing works is to monitor the forwarding behaviors of sensor nodes, which can provide evidence and guidance for attack detection and defense [11]. In the following literature review, the existing work is divided into two categories: acknowledgment based and neighbor surveillance based schemes, according to different monitoring techniques for data forwarding. This type of schemes is to use acknowledgments from different nodes in the routing path to determine the packet loss rate of each hop and detect the attackers [12]. Xiao et al. [13] propose a scheme that randomly chooses a number of intermediate nodes along a forwarding path as checkpoints to return acknowledgments for each received packet. If suspicious behavior is detected, it generates an alarm packet and delivers it to the source node.

Shakshuki et al. [14] design and implement an intrusion-detection system, named Enhanced Adaptive ACKonwledgment (EAACK), for mobile ad hoc networks. Due to the high load of hop-by-hop acknowledgments, EAACK combines a two-hop acknowledgment scheme and an end-to-end acknowledgment scheme to detect the malicious behaviors and reduce the network overhead. In addition, EAACK adopts a digital signature with acknowledgment to ensure authentication, integrity, and non-repudiation. As an elastic evaluation scheme, reputation system is also applied to attack detection.

Zhang et al. [15] develop an audit-based misbehavior detection system to integrate reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavior audits in ad hoc networks. In the correlations between link errors and malicious drops are investigated to detect selective forwarding attacks. In order to guarantee truthful calculation for the correlations, they propose a Homomorphic Linear Authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of acknowledgments reported by nodes.

With the Watchdog hardware [16], sensor nodes can monitor the forwarding behaviors of their neighboring nodes and record the actual packet loss accurately. Suat Ozdemir [5] investigates a functional reputation based reliable data aggregation method against selective forwarding attacks in clustered WSNs. Each node maintains a reputation table to evaluate the behaviors of its neighbor nodes, based on the forwarding monitoring of the neighboring nodes. The nodes with low reputation values are isolated from the routing path. However, the reputation evaluation is only based on the monitored packet loss during the forwarding.

Hao et al. [6] design a repeated game based approach to analyze the collusion on selective forwarding attacks in multi-hop wireless networks. In [17], Li et al. propose a Side Channel Monitoring (SCM) scheme to detect selective forwarding attacks in wireless ad hoc networks. SCM use the nodes adjacent to a data communication route, to constitute a side channel for monitoring the forwarding behaviors of the nodes en route. Once misbehaviors are detected, the monitoring nodes send alarm packets to the source node through both channels. Besides these two categories of countermeasures, multi-path routing is also a widely applied technique to minimize the impact of selective forwarding attacks on data delivery rather than detect nodes.

In wireless sensor network domain, secure data aggregation problem is studied extensively. In [3], the security mechanism detects node misbehaviors such as dropping or forging messages and transmitting false data. In [11], random sampling mechanisms and interactive proofs are used to check the correctness of the aggregated data at base station. In [10], sensor nodes first send data aggregators the characteristics of their data to determine which sensor nodes have distinct data and then those sensor nodes having distinct data send their encrypted data. In [13], the witness nodes of data aggregators also aggregate data and compute MACs to help verify the correctness of the aggregators' data at base station. Because the data validation is performed at base station, the transmission of false data and MACs up to base station affects adversely the utilization of sensor network resources. In [14], sensor nodes use the cryptographic algorithms only when a cheating activity is detected. Topological constraints are introduced to build a Secure Aggregation Tree (SAT) that facilitates the monitoring of data aggregators. In SAT, any child node is able to listen to the incoming data of its parent node. When the aggregated data of a data aggregator are questionable, a weighted voting scheme is employed to decide whether the data aggregator is properly behaving or cheating.

There are centralized trust based systems for Internet such as [18,19]. These systems keep reputation values at a centralized trusted authority and therefore they are not feasible in wireless sensor network domain. Decentralized trust development systems are studied in mobile and ad hoc networks [20–22]. These trust development systems are game theory based and try to counter selfish routing misbehavior of nodes by enforcing nodes to cooperate with each other. An information theoretic trust framework for ad hoc networks is proposed in [24]. The main idea of this work is that trust represents uncertainty that in turn can be computed using entropy. Authors introduce the notion of ‘‘confidence of belief" to separate long-term and short-term trust levels. In another work [23], the transitivity of trust without prior knowledge is used to establish a relation between two entities. In this context, authors map the trust evaluation issue as a path problem on a directed graph. In [25], authors argue that the traditional notion of trust as a relation among entities

All rights reserved by *www.ijsrd.com*

becomes insufficient for emerging data-centric mobile ad hoc networks.

III. CHANNEL AWARE DETECTION AND REPUTATION

Channel Aware detection and reputation is the basic mechanism to evaluate the threshold detection.

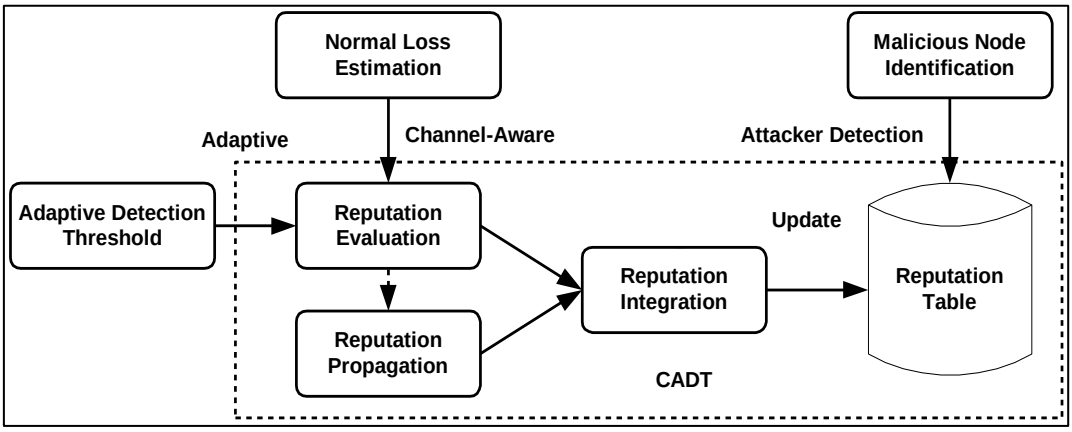

Fig. 1 Proposed Architecture of CADT

Fig. 1 shows the channel aware reputation system which is used to identify the loss of channel and to identify the malicious node using reputation table. The proposed system consists of reputation evaluation, propagation, and integration among the nodes for adaptive channel and to detect the attacker in wireless sensor networks. Based on the node evaluation among the clusters, loss estimation will be calculated based on adaptive channel and the reputation integration are used to identify the malicious node and to detect the attacker.

The proposed system is sub divided into four works namely

1) Network Formation
2) Reputation Update
3) Malicious Nodes Identification
4) Performance Evaluation

A. Network Formation

WSN consisting of a set of randomly distributed sensor nodes, denoted by N, and a sink node to monitor an open area is considered. Each sensor node periodically senses the interested information from the surroundings, and transmits the sensed data to the sink via multi-hop routing among sensor nodes. Sensor nodes communicate with their neighboring nodes based on the IEEE 802.11 DCF. The monitored area has an unstable radio environment, making the packet loss rates during the communications of sensor nodes significantly increased and vary from time to time. Since sensor nodes are deployed in open area and lack adequate physical protection, they may be compromised by adversaries through physical capture or software vulnerabilities to misbehave in data forwarding. Fig. 2 represents the network evaluation time for transmitting messages and evaluate for forwarding attacks.

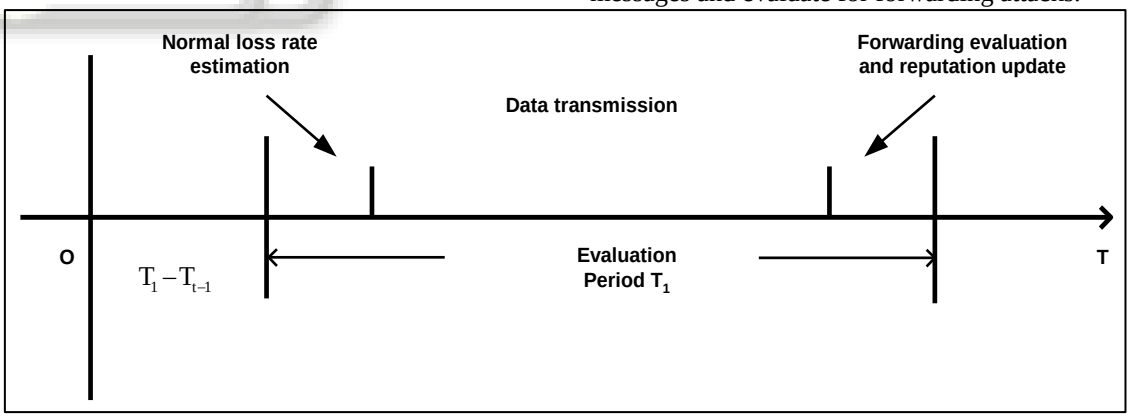

Fig. 2: Network Evaluation Time for Transmitting Messages

B. Reputation Update

The reputation update in CADT consists of three procedures: reputation evaluation, propagation and integration. Reputation Evaluation is to evaluate short-term reputation scores for the forwarding behaviors of sensor nodes, based on the deviation of estimated normal packet loss rate and monitored the actual packet loss rate. With Reputation Propagation, the evaluated short-term reputation scores can be propagated within the neighboring nodes to achieve a more comprehensive evaluation. Finally, by Reputation Integration, sensor nodes integrate the reputation scores evaluated by them and the propagated reputation scores from their neighboring nodes to update the reputation table. To reduce the routing overhead and updates in routing table $p_{i,j}$ is the coincidence factor to avoid overlapping, and the respective formula is given by

$$\text{Minimize } V_j = P_j \cdot \eta_{i,j}(t) + (1 - p_j) \cdot \mu_{i,j}(t)$$

$$\text{s.t. } \begin{cases} p_{i,j}(t) \cdot S_i(t) < \xi_{i,j}(t) < S_i(t) \\ \xi_{i,j}(t) \in N^+ \end{cases}$$

All rights reserved by *www.ijsrd.com*

C. Malicious Nodes Identification

Each compromised sensor nodes can launch selective forwarding attacks to degrade the performance of the network. Specifically, when a compromised sensor node receives a data packet, it maliciously drops it with a probability, referred to as attack probability. Since the adversary can control the attack probabilities of compromised nodes, it is difficult to distinguish if the packet losses are caused by fluctuated channel condition or malicious drops, especially for the nodes with low attack probabilities. Fig. 3 represents the drop identification between malicious, Normal drop as well as No loss in transmission.

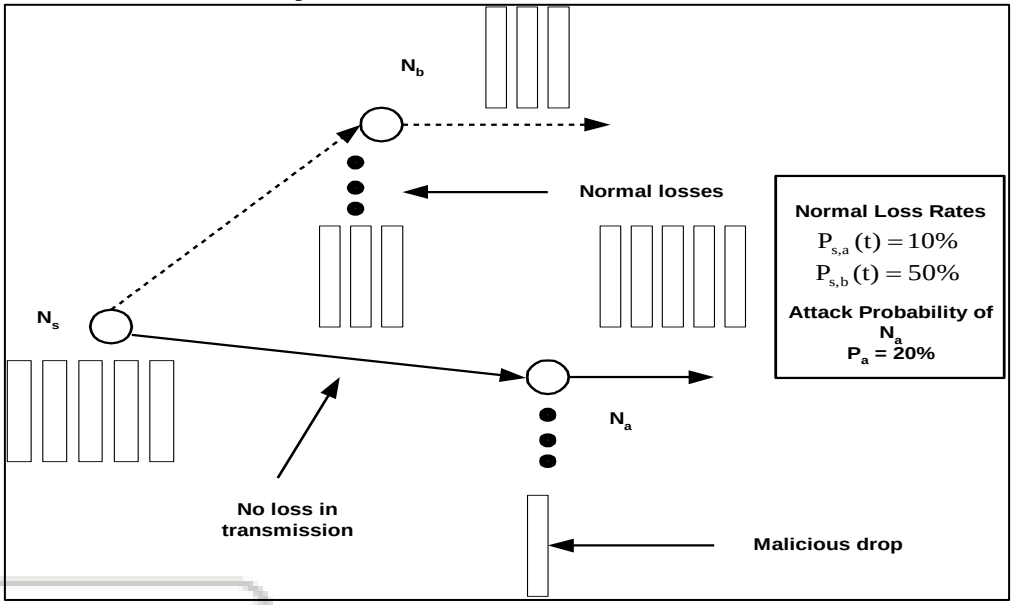

Fig. 3: Drop Identification between Malicious, Normal Drop and No Loss in Transmission

D. Performance Evaluation

1) Detection accuracy:

High detection accuracy should be achieved for detecting selective forwarding attacks and identifying the malicious nodes, which can be measured by two metrics. The one is the attacks should be accurately detected once the malicious nodes misbehave in data forwarding. The other is normal nodes cannot be falsely detected as malicious nodes due to the fluctuated normal packet losses. To identify the optimum threshold level p_j be the factor for sensing the different threshold values and $[a]^+$ be the attack probabilities for nodes

$$P_j = \left\lfloor \frac{\sum_{w=0}^{t} \left[m_{i,j}(w) - S_{i,j}(w) \cdot (1 - p_{i,j}(w)) \right]}{\sum_{w=0}^{t} \left[S_{i,j}(w) \cdot (1 - p_{i,j}(w)) \right]} \right\rfloor^{+},$$

where $[a]^+ = a$, if $a \geq 0$; otherwise, $[a]^+ = o$

2) Data delivery Ratio Improvement:

Besides the detection of selective forwarding attacks, the data delivery ratio of the network should be improved by the proposed scheme to mitigate the negative impacts caused by the attacks. Meanwhile, the proposed scheme should be able to partly stimulate the cooperation of malicious nodes in data forwarding.

IV. PERFORMANCE ANALYSIS

The delay interval between the source to destination between CADT and AODV protocol is observed in various ratio of malicious node as shown in Fig. 4. CADT has the delay lesser than AODV protocol.

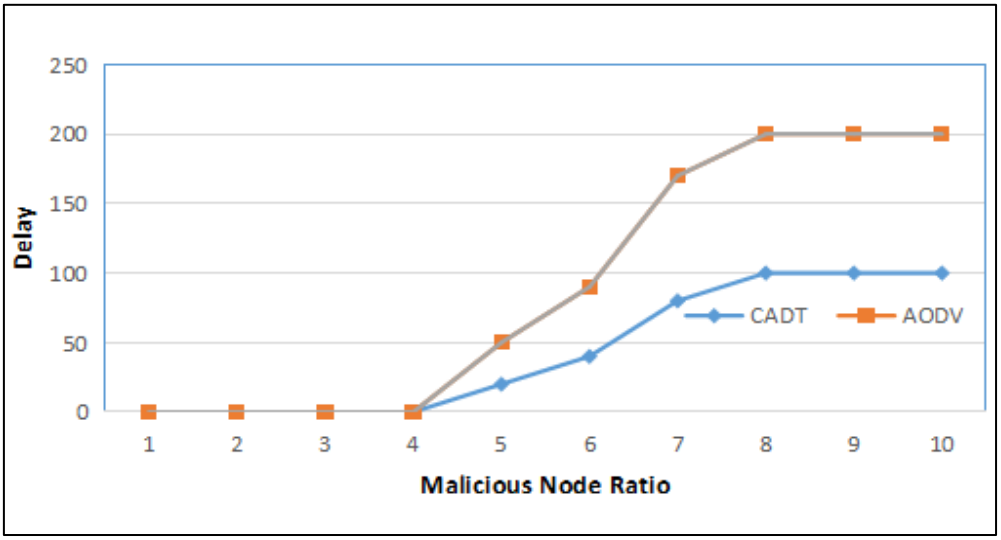

Fig. 4: Observed Delay

All rights reserved by *www.ijsrd.com*

The throughput of AODV and CADT protocol is observed in various speeds. CADT has a higher throughput than AODV as shown in Fig. 5.

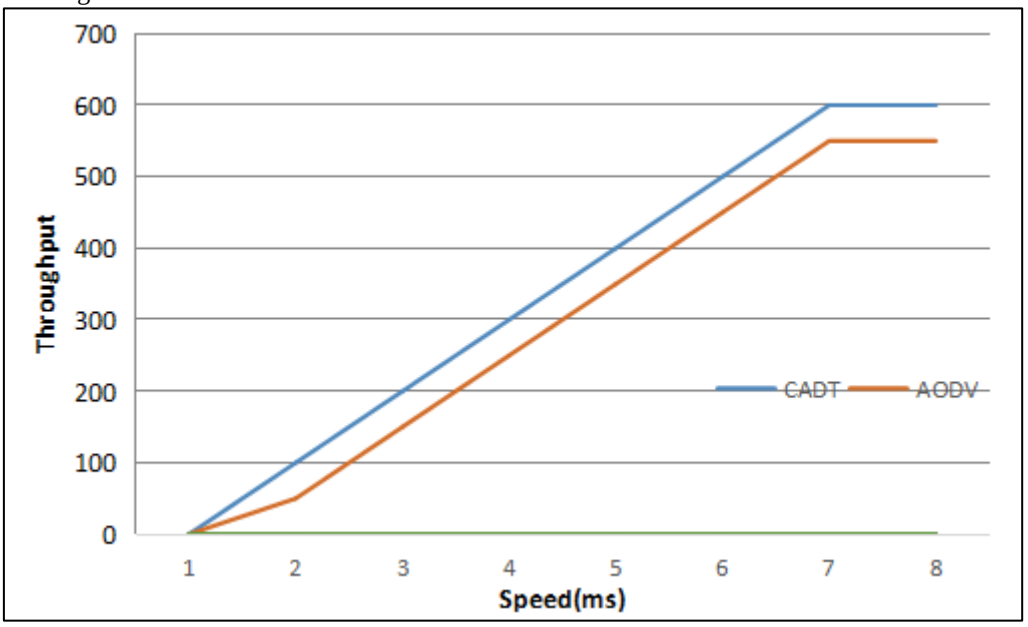

Fig. 5: Observed Throughput

V. Conclusion

A Channel-Aware Reputation System with Adaptive Detection Threshold (CADT) to detect selective forwarding attacks in WSNs is proposed. To accurately distinguish selective forwarding attacks from the normal packet loss, CADT evaluates the forwarding behaviors by the deviation between the estimated normal packet loss and monitored packet loss. To improve the detection accuracy of CADT, the optimal evaluation threshold of CADT in a probabilistic way is derived, which is adaptive to the time-varied channel condition and the attack probabilities of compromised nodes. In addition, a distributed and attack-tolerant data forwarding scheme is developed to collaborate with CADT for stimulating the cooperation of compromised nodes and improving the data delivery ratio. The simulation results show that the proposed CADT can achieve high detection accuracy with low false and missed detection probabilities, and the proposed attack tolerant data forwarding scheme can improve more than 10% data delivery ratio for the network.

References

[1] Butun, S. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks", IEEE Commun. Surv. & Tutor., vol. 16, no. 1, pp. 266–282, 2014.
[2] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks", IEEE Trans. Commun., vol. 61, no. 12, pp. 5103–5113, 2013.
[3] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify suspect nodes in selective forwarding attacks", J. Parallel Distributed Comput., vol. 67, no. 11, pp. 1218–1230, 2007.
[4] "The Network Simulator NS2", [Online]. Available: http://www.is.edu/nsnam/ns/.
[5] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks", Comput. Commun., vol. 31, no. 17, pp. 3941–3953, 2008.
[6] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, "A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks", Comput. Commun., vol. 35, no. 17, pp. 2125–2137, 2012.
[7] X. Liang, X. Lin, and X. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks", IEEE Trans. Parallel Distr. Sys., vol. 25, no. 2, pp. 310–320, 2014.
[8] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Sacrm: Social aware crowd sourcing with reputation management in mobile sensing", Computer Commun., vol. 65, no. 15, pp. 55–65, 2015.
[9] L. Yu, S. Wang, K. Lai, and Y. Nakamori, "Time series forecasting with multiple candidate models: selecting or combining", J. Sys. Sci. Complexity, vol. 18, no. 1, pp. 1–18, 2005.
[10] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting channel-aware reputation system against selective forwarding attacks in WSNs", In Proc. IEEE GLOBECOM, 2014, pp. 330–335.
[11] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges", IEEE Commun. Surv. & Tutor., vol. 13, no. 4, pp. 658–672, 2011.
[12] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in Manets", IEEE Trans. Mob. Comput., vol. 6, no. 5, pp. 536–550, 2007.
[13] E. Mahmoud and X. Shen, "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks", IEEE Trans. Vehic. Tech., vol. 60, no. 8, pp. 3947–3962, 2011.
[14] E. Shakshuki, N. Kang, and T. Sheltami, "Eaacka secure intrusion detection system for Manets", IEEE

All rights reserved by *www.ijsrd.com*

Trans. Ind. Electro., vol. 60, no. 3, pp. 1089–1098, 2013.
[15] T. Shu and M. Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing", In Proc. ACM WiSec, 2012, pp. 87–98.
[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In Proc. ACM MobiCom, 2000, pp. 255–265.
[17] X. Li, R. Lu, X. Liang, and X. Shen, "Side channel monitoring: packet drop attack detection in wireless ad hoc networks", In Proc. IEEE ICC, 2011, pp. 1–5.
[18] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNS", IEEE Trans. Wirel. Commun., vol. 9, no. 5, pp. 1661–1675, 2010.
[19] Q. Liu, J. Yin, V. Leung, and Z. Cai, "Fade: Forwarding assessment based detection of collaborative grey hole attacks in WMNS", IEEE Trans. Wirel. Commun., vol. 12, no. 10, pp. 5124–5137, 2013.
[20] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Exploiting mobile crowdsourcing for pervasive cloud services: challenges and solutions", IEEE Commun. Mag., vol. 53, no. 3, pp. 98–105, 2015.
[21] Nadeem and M. P. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks", IEEE Commun. Surv. & Tutor., vol. 15, no. 4, pp. 2027–2045, 2013.
[22] H. Lin, X. Zhu, Y. Fang, D. Xing, C. Zhang, and Z. Cao, "Efficient trust based information sharing schemes over distributed collaborative networks", IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 279–290, 2013.
[23] J. Tang, Y. Cheng, and W. Zhuang, "Real-time misbehavior detection in IEEE 802.11-based wireless networks: An analytical approach", IEEE Trans. Mob. Comput., vol. 13, no. 1, pp. 146–158, 2014.
[24] T. Liu and A. E. Cerpa, "Data-driven link quality prediction using link features", ACM Transactions on Sensor Networks (TOSN), vol. 10, no. 2, p. 37, 2014.
[25] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function", IEEE J. Sel. Areas Commun., vol. 18, no. 3, pp. 535–547, 2000.

All rights reserved by *www.ijsrd.com*