ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Issue 5, May 2017

Novel Detection of Selective Forwarding Attacks Using CRS-A

B.Balakumar[1], K.S. Saji[2]

[1]Assistant Professor, Centre for Information Technology and Engineering,
Manonmaniam Sundaranar University, Tirunelveli, India, balakumarmsu@gmail.com

[2]PG Student - M.Tech., Centre for Information Technology and Engineering,
Manonmaniam Sundaranar University, Tirunelveli, India,
sajiks123@gmail.com

Abstract- In this system, we have proposed a channel-aware reputation system with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. To accurately distinguish selective forwarding attacks from the normal packet loss, CRSA evaluates the forwarding behaviors by the deviation between the estimated normal packet loss and monitored packet loss. To improve the detection accuracy of CRS-A, we have further derived the optimal evaluation threshold of CRS-A in a probabilistic way, 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 CRS-A for stimulating the cooperation of compromised nodes and improving the data delivery ratio. Our simulation results show that the proposed CRS-A can achieve a 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. In our future work, we will extend our investigation into WSNs with mobile sensor nodes, where the detection of selective forwarding attacks becomes more challenging, since the normal packet loss rate is more fluctuant and difficult to estimate due to the mobility of sensor nodes.

Keywords- ***CRS-A, Data Delivery Ratio, WSN.***

1. INTRODUCTION

Most of related works focus on monitoring the packet losses in each transmission link and isolating the nodes with high packet loss rates from the data forwarding path. These solutions can improve the data delivery ratio or network throughput but have little effect on detecting selective forwarding attacks. Since the main challenge of attack detection is to distinguish the malicious drop from normal packet loss, the normal packet loss rate of the transmission link should be considered in the forwarding evaluation. For example, a source node Ns sends 10 packets to the destination node Nd via two forwarding nodes Na and Nb, respectively. Na forwards 6 packets to Nd, while Nb only forwards 5 packets to Nd. Intuitively, Na behaves better than Nb during the data forwarding. However, if the normal packet loss rates from Ns to Na and Nb are 20% and 50%, respectively, Na should have a higher probability to misbehave in this data forwarding. Therefore, we consider the deviation between the normal losses and actual losses as the key factor to detect selective forwarding attacks.

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. 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 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 system, we propose a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. Specifically, we divide the network lifetime to a sequence of evaluation periods.1 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 CRS-A. Once the reputation value of a senor node is below an alarm value, it would be identified as a compromised node by CRS-A. Compared to our previous work, this system has the following enhancements and new contributions.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Issue 5, May 2017

(i) We propose CRS-A, which evaluates the forwarding behaviors of sensor nodes by utilizing an adaptive detection threshold. By theoretically analyzing its performance, we derive an optimal detection threshold for evaluating the forwarding behaviors to optimize the detection accuracy of CRS-A. The optimal detection threshold is determined for each transmission link in a probabilistic way, and can also be adaptive to the time-varied channel condition and the attack probability of the forwarding node.
(ii) We develop a distributed and attack-tolerant data forwarding scheme to collaborate with CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data delivery ratio of the network. Rather than isolating all the compromised nodes from data forwarding, it jointly considers the time-varied channel condition and attack probabilities of neighboring nodes in choosing forwarding nodes.
(iii) Extensive simulation results demonstrate that the proposed CRS-A with attack-tolerant data forwarding scheme can achieve a high detection accuracy with both of false and missed detection probabilities close to 0, and improve more than 10% data delivery ratio for the network.

Due to their high-energy efficiency, a low temperature (60–80C) operation, a pollution-free character, and a relatively simple design the PEM fuel cells are currently being considered as an alternative source of power in the electric vehicles. However, further improvements in the efficiency and the cost are needed before the PEM fuel cells can begin to successfully compete with the traditional internal combustion engines. The development of the PEM fuel cells is generally quite costly. Fuel cells in the range of 1W-100kW range are being considered for near term service in several remote and mobile applications where they provide quiet operation, high reliability, potentially high energy density and ultra-low emissions. In recent years, research and development in fuel cells and fuel cell systems have accelerated, and although significant improvements in polymer electrolyte membrane fuel cell technology has been achieved over the past decade, the performance, stability, and reliability for today's fuel cell technology is not sufficient to replace internal combustion engines. On the other hand, the cost of fuel cell systems is still too high for them to become viable commercial products. In a PEM fuel cell stack, the cells are electrically connected in series and the polarization curves of the individual cells can be measured by measuring the current of the entire stack and the voltages of individual cells.

II. LITERATURE REVIEW

Wireless sensor networks (WSNs) are vulnerable to selective forwarding attacks that selectively drop a subset of the forwarding packets to degrade network performances. Due to unstable wireless channels, the packet loss rate between sensor nodes might be high, especially in hostile environments. Therefore, it is difficult to distinguish the malicious drop and normal packet loss. In this paper, we propose a Channel-aware deputation System (CRS) to identify selective forwarding misbehaviours from normal packet losses caused by poor channel quality or medium access collision. Specifically, CRS is based on normal packet loss estimation and neighbour monitoring. Each node maintains a reputation table to evaluate forwarding behaviours of its neighbours. Reputation value is determined by the deviation of the monitored packet loss rate and estimated normal loss rate. The nodes with reputation below a threshold are identified as misbehaving nodes and isolated from data forwarding paths. Furthermore, we develop weighted reputation propagation and integration functions to improve detection efficiency. Through theoretical analysis and extensive simulations, we demonstrate that CRS can accurately detect selective forwarding attacks and significantly improve the network throughput.

In mobile ad hoc networks (MANETs), nodes usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehavior is generally referred to as packet dropping attack or black hole attack, which is considered as one of the most destructive attacks that leads to the network collapse. The special network characteristics, such as limited battery power and mobility, make the prevention techniques based on cryptographic primitives ineffective to cope with such attack. Rather, a more proactive alternative is required to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Once such scheme fails, some economic-based approaches can be adopted to alleviate the attack consequences by motivating the nodes cooperation. As a backup, detection and reaction schemes remain as the final defense line to identify the misbehaving nodes and punish them. In this paper, we make a comprehensive survey investigation on the state-of-the-art countermeasures to deal with the packet dropping attack. Furthermore, we examine the challenges that remain to be tackled by researchers for constructing an in-depth defense against such a sophisticated attack. [5] proposed a system which is an innovative congestion control algorithm named FAQ-MAST TCP (Fast Active Queue Management Stability Transmission Control Protocol) is aimed for high-speed long-latency networks. Four major difficulties in FAQ-MAST TCP are highlighted at both packet and flow levels. The architecture and characterization of equilibrium and stability properties of FAQ-MAST TCP are discussed. Experimental results are presented comparing the first Linux prototype with TCP

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Issue 5, May 2017

Reno, HSTCP, and STCP in terms of throughput, fairness, stability, and responsiveness. [6] proposed a system in which FASTRA downloads and data transfers can be carried over a high speed internet network. On enhancement of the algorithm, the new algorithm holds the key for many new frontiers to be explored in case of congestion control.

III. SYSTEM DESIGN

A. System Architecture

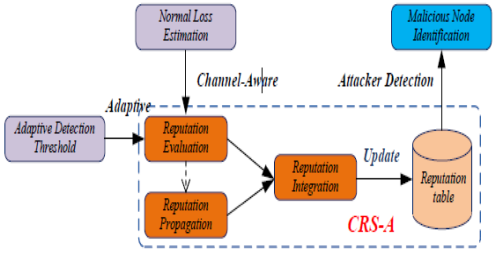

Fig.2. System Architecture

B. Coding

```
setval(chan)        Channel/WirelessChannel    ;
setval(prop)        Propagation/TwoRayGround   ;
setval(netif)       Phy/WirelessPhy            ;
setval(mac)         Mac/802_11                 ;
setval(ifq)         Queue/DropTail/PriQueue    ;
setval(ll)          LL                         ;
setval(ant)         Antenna/OmniAntenna        ;
setval(ifqlen)      1000                       ;
setval(nn)          33                         ;
setval(rp)          AODV                       ;
setval(x)    700
setval(y)    700
set ns_      [new Simulator]

set F1ab 38;
set D 17;
set M 26;
set R 15;
set e_0 3.5;
set f [open Trace.tr w]
$ns_ trace-all $f
$ns_ use-newtrace
setnamtrace [open Nam.nam w]
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)

set topo      [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)

set chan_1_ [new $val(chan)]
set chan_2_ [new $val(chan)]

set chan_1_ [new $val(chan)]
set chan_2_ [new $val(chan)]
$ns_ node-config -adhocRouting $val(rp) \
      -llType $val(ll) \
      -macType $val(mac) \
      -ifqType $val(ifq) \
      -ifqLen $val(ifqlen) \
      -antType $val(ant) \
      -propType $val(prop) \
      -phyType $val(netif) \
      -topoInstance $topo \
      -agentTrace ON \
      -routerTrace ON \
      -macTrace ON \
      -movementTrace ON \
      -channel $chan_1_
$ns_ node-config \      channel $chan_2_

procNoOfNodes { } {
      puts "\nEnter Number of
Nodes\n**********************************
\n"
         setchk 1
         while { $chk==1 } { puts "Enter No. of Nodes
between 40 and 60 :"  ; set d [gets stdin]
                  if { $d >=40 && $d<=60 } { set chk 0 }
else {  puts " Wrong input !!!" } }
         if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }

set n [NoOfNodes]
```

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Issue 5, May 2017

```
set n [expr ($n-1)]



procSrcNode { } {
      global n
      puts "\nSource
Node\n*************************\n"
         setchk 1
         while { $chk==1 } {

         set S1 [expr ($n-20)]
         puts "Enter the Source Node between 10 and
$S1 :";

         set d [gets stdin]
                  if { $d >=10 && $d<=$S1 } { set chk 0 }
else {  puts " Wrong input !!!" } }
         if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }

setSrc [SrcNode]



procDestNode { } {
      global n
      globalSrc
      puts "\nDestination
Node\n*************************\n"
         setchk 1
         while { $chk==1 } {

         set D1 [expr ($Src+5)]
         set D1x [expr ($Src+2)]

         set D2 [expr ($Src+10)]

         if { ($D2>$n) } { set D1 $D1x; set D2 $n; }

         puts "Enter the Destination Node between $D1
and $D2 :";

         set d [gets stdin]
                  if { $d >=$D1 && $d<=$D2 } { set chk
0 } else {  puts " Wrong input !!!" } }
         if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }
setDest [DestNode]
setSinkNode [expr ($Dest+2)]

procTransPacketSize { } {
      puts "\nTransmission Packet Size in
bytes\n************************************\
n"
         setchk 1
         while { $chk==1 } { puts "Enter Packet Size
between 2312 and 2500 :"  ; set d [gets stdin]
                  if { $d >=2312 && $d<=2500 } { set
chk 0 } else {  puts " Wrong input !!!" } }
         if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }

procIndiEnergyLevel { } {
      puts "\nIndividual Battery Energy
Level\n*************************\n"
         setchk 1
         while { $chk==1 } { puts "Enter your choice
between 100 and 200 :"  ; set d [gets stdin]
                  if { $d >=100 && $d<=200 } { set chk 0
} else {  puts " Wrong input !!!" } }
         if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }
procPackTransSpeed { } {
      puts "\nPackets Transmission
Speed\n******************\n"
         setchk 1
         while { $chk==1 } { puts "Enter your choice
between 30 and 70 bps :"  ; set d [gets stdin]
```

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Issue 5, May 2017

```
        if { $d >=30 && $d<=70 } { set chk 0 } else {
puts " Wrong input !!!" } }
        if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }
procNodeMobility { } {
      puts "\nNode Mobility Speed(Threshold
value)\n************************************
*\n"
        setchk 1
        while { $chk==1 } { puts "Enter Mobility Speed
between 100 and 500 :"  ; set d [gets stdin]
        if { $d >=100 && $d<=500 } { set chk 0 } else {
puts " Wrong input !!!" } }
        if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }
procTransmissionRange { } {
      puts "\nTransmission Range (Threshold
value)\n************************************
*\n"
        setchk 1
        while { $chk==1 } { puts "Enter your choice
between 20 and 30 M :"  ; set d [gets stdin]
        if { $d >=20 && $d<=30 } { set chk 0 } else {
puts " Wrong input !!!" } }
        if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }
procPacketsDroppingRate { } {
      puts "\nPackets Dropping Rate (Threshold
value)\n************************************
*\n"
        setchk 1
        while { $chk==1 } { puts "Enter your choice
between 10 and 20 bps :"  ; set d [gets stdin]
        if { $d >=10 && $d<=20 } { set chk 0 } else {
puts " Wrong input !!!" } }
        if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }
procAverageTransmissionDelay { } {
      puts "\nAverage Transmission Delay (Threshold
value)\n************************************
*\n"
        setchk 1
        while { $chk==1 } { puts "Enter your choice
between 5 and 10 ms :"  ; set d [gets stdin]
        if { $d >=5 && $d<=10 } { set chk 0 } else {  puts
" Wrong input !!!" } }
        if { ($chk==1) } { puts "\n Wrong Choice. Try
Again !!! \n\n" ; exit 0 }
   return $d
            }
set sq3 [TransPacketSize]

Agent/TCP set packetSize_ $sq3
set tcp31 [new Agent/TCP]
$tcp31 set class_ 2
set sink31 [new Agent/TCPSink]
$ns_ attach-agent $node_($Nr8) $tcp31
$ns_ attach-agent $node_($Nr9) $sink31
$ns_ connect $tcp31 $sink31
set ftp31 [new Application/FTP]
$ftp31 attach-agent $tcp31
$ns_ at 75.6 "$ftp31 start"
$ns_ at 89.5 "$ftp31 stop"
$ns_ at 75.6 "$node_($Nr9) label NN"
$ns_ at 75.6 "$node_($Nr9) add-mark m0 cyan"
$ns_ at 75.6 "$node_($Nr9) color cyan"

Agent/TCP set packetSize_ $sq3
set tcp31 [new Agent/TCP]
$tcp31 set class_ 2
set sink31 [new Agent/TCPSink]
$ns_ attach-agent $node_($Nr9) $tcp31
$ns_ attach-agent $node_($SinkNode) $sink31
$ns_ connect $tcp31 $sink31
set ftp31 [new Application/FTP]
$ftp31 attach-agent $tcp31
$ns_ at 89.6 "$ftp31 start"
$ns_ at 98.0 "$ftp31 stop"
```

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 3, Issue 5, May 2017

```
Agent/TCP set packetSize_ $sq3
set tcp31 [new Agent/TCP]
$tcp31 set class_ 2
set sink31 [new Agent/TCPSink]
$ns_ attach-agent $node_($SinkNode) $tcp31
$ns_ attach-agent $node_($Dest) $sink31
$ns_ connect $tcp31 $sink31
set ftp31 [new Application/FTP]
$ftp31 attach-agent $tcp31
$ns_ at 89.6 "$ftp31 start"
$ns_ at 98.0 "$ftp31 stop"
}
for {set i 0} {$i< $n} {incri} {
   $ns_ at 99.0 "$node_($i) reset";
}
$ns_ at 99 "stop"
$ns_ at 99 "puts \"Simulation Ends...\" ; $ns_ halt"
proc stop {} {
global ns_ namtrace  node_ sq1 sq2
   $ns_ flush-trace
close $namtrace
   exec ./nam -r 2m Nam.nam&
}
puts "Starting Simulation..."
$ns_ run
```

IV. CONCLUSION

In this system, we have proposed a channel-aware reputation system with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. To accurately distinguish selective forwarding attacks from the normal packet loss, CRSA evaluates the forwarding behaviors by the deviation between the estimated normal packet loss and monitored packet loss. To improve the detection accuracy of CRS-A, we have further derived the optimal evaluation threshold of CRS-A in a probabilistic way, 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 CRS-A for stimulating the cooperation of compromised nodes and improving the data delivery ratio. Our simulation results show that the proposed CRS-A can achieve a 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. In our future work, we will extend our investigation into WSNs with mobile sensor nodes, where the detection of selective forwarding attacks becomes more challenging, since the normal packet loss rate is more fluctuant and difficult to estimate due to the mobility of sensor nodes.

REFERENCES

[1] I. 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] Y. Zhang, L. Lazos, and W. Kozma, "Amd: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mob. Comput.,prePrints, published online in Sept. 2013.

[5] Christo Ananth, S.Esakki Rajavel, I.AnnaDurai, A.Mydeen@SyedAli, C.Sudalai@UtchiMahali, M.Ruban Kingston, "FAQ-MAST TCP for Secure Download", International Journal of Communication and Computer Technologies (IJCCTS), Volume 02 – No.13 Issue: 01 , Mar 2014, pp 78-85.

[6] Christo Ananth, A. Ramalakshmi, S. Velammal,B. Rajalakshmi Chmizh, M. Esakki Deepana, "FASTRA –SAFE AND SECURE", International Journal For Technological Research In Engineering (IJTRE), Volume 1, Issue 12, August-2014,pp: 1433-1438.

[7] R.B. Bird, W.E. Stewart, E.N. Lightfoot, Transport Phenomena, Wiley, New York, 1960.