Computer Security Symposium 2020
26 - 29 October 2020

AODV環境における信頼度評価の精度向上に関する研究

曺 智雄[1,a)]　中村 康弘[1]

概要：モバイルアドホックネットワークでは，中央集権的なコントローラがなく，マルチホップ方式の通信を行うためパケット消失に脆弱である．そのため，隣接ノードのパケット転送を監視してそのノードに対する信頼度 (Trust) を評価し，ルーティングに活用するセキュアルーティングプロトコルが提案されている．しかし，無線環境のさまざまな要因により，送信者ノードだけでは経路に対する正確な信頼度評価が困難である．そこで，本稿では信頼度モデルに機械学習を適用し，信頼度評価の精度を向上させる手法を提案する．この手法は不正ノードの存在や無線環境の変化に追随し，動的に再評価を繰り返す．そしてns-3 シミュレータ上に実装を行い，既存手法と比較評価を行なってその有効性を確認した．

キーワード：trust-based routing, aodv, machine learning, ns3, manet

An Improvement Method for Trust Evaluation in AODV Environment

Jiwoong Cho[1,a)]　Yasuhiro Nakamura[1]

Abstract: Mobile ad hoc networks are vulnerable to packet loss because they do not have a centralized controller and communicate in a multi-hop routing environment. For this reason, a secure routing protocol has been proposed to evaluate the trustworthiness of neighboring nodes by monitoring their packet transmissions and utilizing it for routing. However, due to various factors in the wireless environment, it is difficult to accurately evaluate the reliability of the route by the sender. In this paper, we propose a method to improve the accuracy of trust evaluation by applying machine learning to the trust models. This method is utilized to the presence of malicious nodes and changes in the radio environment, and reevaluates them dynamically. The method is implemented on the ns-3 simulator and compared it with existing methods to confirm its effectiveness.

Keywords: CSS 2020, LaTeX, style files

1. はじめに

近年，モバイルアドホックネットワーク (MANET) に関する様々な研究がなされている [1]．MANET は中央集権的なコントローラが不在 [2] する環境でノード同士が協力して構築するネットワークであり，従来のインフラストラクチャ型ネットワークの展開が困難な場面において重要な役割を果たしている．しかし，MANET はリソースに制約のあるノード同士が移動しながら無線通信を行うため，インフラストラクチャ型ネットワークより不安定でパケット損失が多発する．そのため，隣接ノードのパケット転送動作 (Forwarding) を監視して信頼度 (Trust) を評価し，それを用いてより安定した経路を構築するセキュアルーティングプロトコル (SRP) が提案されている．

しかし，ルーティングプロトロルがネットワーク層 (L3) に分類されているが，そのプロトコルの精度は下層 (L1, L2) の不具合など様々な要因により多く影響される．そのため，プロミスキャスモード [3] であっても隣接ノードによるパケット転送の補足に失敗する場合がある．そのため，ネットワーク中に悪意ノード (Malicious Node) ではないにもかかわらず，隣接ノードに対する信頼度がかなり低く評価されて，経路発見 (Route Discovery) 自体が不能になる場合も発生することをシミュレーション実験を通して確

[1] 防衛大学校理工学研究科
Graduate School of Science and Engineering, National Defense Academy of Japan
[a)] jiwoong6830@gmail.com

認した．

そこで，本稿では信頼度評価モデルに機械学習 (Machine Learning)[4] を応用して，周りの環境変化に追随する手法を提案する．そして従来のノード信頼度評価モデル (Node Trust Model) に新たな環境変数 (E_{CFR}，E_{DFR}) を導入し，隣接ノードごとに環境変化を評価してノード信頼度評価モデルを学習させる．これを周期的に行うことにより，周りの通信環境に合わせてモデルを随時変化させていく．

以下本稿では，２章において関連研究について述べ，３章では提案手法ついて，４章ではシミュレーション実装及び評価により提案手法の有効性を示す．最後に５章では結論を述べる．

2. 関連研究

2.1 AODV と信頼度評価

MANET 環境におけるルーティングプロトコルはプロアクティブ型とリアクティブ型に分類される．プロアクティブ型プロトコルはユーザーが通信する前から経路を発見して維持することにより，通信要求から実際の通信までの時間を大幅に短縮する．リアクティブ型プロトコルはユーザーが通信を要求してから経路発見を行うため，通信要求から実際の通信までは多少時間はかかるが，MANET 環境における各ノードによるリソースの節約に有利である．

AODV(Ad hoc On-Demand Distance Vector) に信頼度評価を適用する研究は多くなされている．リアクティブ型プロトコルには AODV，DSR，TORA などがある．Pirzada A.A ら [5] はリアクティブ型プロトコルに信頼度評価手法を適用し，ネットワーク負荷が重い環境下でのパフォーマンスを比較評価して，AODV のスループットが最も安定していることを報告した．

それを受け，X.Li ら [6] は AODV に信頼度手法を適用し，新たな制御パケット (RUPD) を用いて経路信頼度を随時アップデートする上で，１回の経路発見で２つの経路を獲得して経路発見数を減らす手法 (AOTDV) を発表した．本稿では AOTDV に提案手法を適用した．

2.2 信頼度評価によるセキュアルーティング

セキュアルーティングプロトコルにおける信頼度評価の手法は多く提案されているが，信頼度評価に主に用いられるのは，ノード信頼度 (Node Trust) と経路信頼度 (Path Trust) である．ノード信頼度は，自分からパケットを受信した隣接ノードが正しく転送する度合いを表す．経路信頼度は経路上のすべてのノード信頼度をかけた値で，この経路を選択する場合，パケットが宛先ノードまでどれほど正しく転送されるかを表す．

2.3 ノード信頼度の算出

$$FR(t) = \begin{cases} \frac{N_C(t)-N_C(t-W)}{N_A(t)-N_A(t-W)} & ,t > W \\ \frac{N_C(t)}{N_A(t)} & ,t \leq W \end{cases} \quad (1)$$

パケット転送率 (Forwarding Ratio, FR) は隣接ノードが受信したパケットを正しく転送する割合を表す．N_C はプロミスキャスモードによって確認したパケット転送数を表し，N_A は送信したすべてのパケット数を表す．W はタイムウィンドウ (Time Window) であり，現時点を基準として W を外れるパケット転送記録は削除されることによって，パケット転送情報を最新状態に維持することができる．

MANET のパケットは制御パケット (Control Packet) とデータパケット (Data Packet) に分類される．AODV において制御パケットは経路発見及び維持などに用いられる RREQ(Route Request), RREP(Route Reply), RERR(Route Error)，RUPD(Route Update) などがある．制御パケットは経路構築に重要な役割を果たすため，信頼度評価における転送率も制御パケット転送率 (Control Packet Forwarding Ratio, $CFR(t)$) とデータパケット転送率 (Data Packet Forwarding Ratio，$DFR(t)$) に分けて考慮する．ノード信頼度は CFR_{jk} と DFR_{jk} に重み定数 ω_{CFR} と $\omega_{DFR}(0 \leq \omega_{CFR}$，$\omega_{DFR}$ and $\omega_{CFR} + \omega_{DFR} = 1)$ を適用して下記のように求める．ここで t は現在の時刻を表す．

$$T_{jk}(t) = \omega_{CFR} \times CFR_{jk}(t) + \omega_{DFR} \times DFR_{jk}(t) \quad (2)$$

2.4 経路信頼度の算出

経路信頼度は各ノードがそれぞれ隣接ノードに対してノード信頼度を算出した上で，経路発見を通して算出される．経路信頼度は下記の式のように，制御パケットが経由する経路上のすべてのノード信頼度をかけて求める [7].

$$T_P(t) = \prod(\{T_{jk}(t) jn_j, n_k \in P \, and \, n_j \rightarrow n_k \, and \, n_k \neq N_d\}) \quad (3)$$

ここで P は経路を表し，n_j，n_k は経路上の隣接ノード関係を表す．$n_j \rightarrow n_k$ は n_k が n_j の次ホップノードであることを表し，N_d は宛先ノードを表す．ここで，宛先ノード N_d の直前に位置するノードは宛先ノードに対するノード信頼度を 1 に設定して経路信頼度求める．その理由は宛先ノードはパケット転送動作を行わないため，ノード信頼度を評価することができないためである．これを図に表したものが図 1 である．

図 1 で T_{AB} はノード A がノード B に対して評価したノード信頼度である．ノード A からノード F までの経路 $P(A, B, E, F)$ の経路信頼度は $0.72(T_{P(A,B,E,F)} = T_{AB} \times T_{BE} = 0.8 \times 0.9 = 0.72)$ になる．ここで，経路 $P(A, B, E, F)$ の中でノード信頼度 T_{EF} は 1 となる．

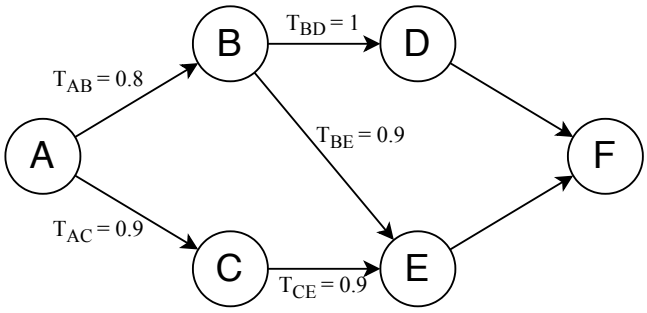

図 1　経路信頼度モデル

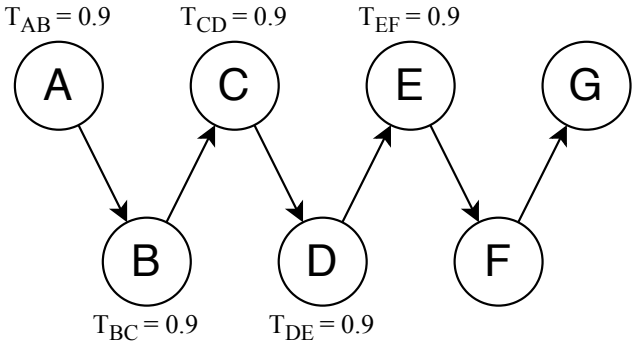

図 2　信頼度評価の精度問題

2.5　TrustRecordList

信頼度評価では従来のルーティングテーブルとは別に信頼度管理のため TrustRecordList を管理する．TrustRecordList は各 TrustRecordListEntry に隣接ノードの ID，ノード信頼度，送受信パケット数，送信したパケット情報などを保存する．

2.6　ノード信頼度評価の精度問題

信頼度評価は最初ノード信頼度が算出され，その結果が経路信頼度につながる仕組みである．それに，信頼度は $[0, 1]$ の連続量であるため，ノード信頼度の誤差は経路信頼度の精度に甚大な影響をもたらす．特に経路のホップ数が長くなればなるほど，経路上の各ノードのわずかな誤差は経路信頼度に指数関数的な誤差をもたらすことになる．図 2 の経路 $P(A, B, C, D, E, F, G)$ を想定して経路信頼度を計算すると，$0.59(T_{P(A,B,C,D,E,F,G)} = T_{AB} \times T_{BC} \times T_{CD} \times T_{DE} \times T_{EF} = 0.9 \times 0.9 \times 0.9 \times 0.9 \times 0.9 = 0.59)$ になる．信頼度評価では閾値 (Threshold) を設定して，ノード信頼度あるいは経路信頼度が閾値より低くなる場合，ネットワークから排除する．信頼度と適切な閾値についての解釈は主観性が強いが，他研究における実験で設定される閾値 [8][9] を参考にすると，0.59 は人間的な感覚からはかなり低いと言える．したがって各ノードが行うノード信頼度評価の精度を向上させることは重要な課題である．

図 3 は ns-3 シミュレータに AOTDV を実装して隣接ノードの実際の転送数とプロミスキャスモードで捕捉した転送数とのズレを確認したグラフである．それぞれ 50 個のノードを一定間隔に固定配置し，1200 秒のシミュレーション時間の間に 1 秒間隔で 1000 個のパケットを送信した．図 3 では，パケット破棄攻撃や伝播損失モデルなど適用せずに普通にパケットを送信しながら送信数，実際の到達数 (転送数)，プロミスキャスモードでキャプチャした転送数を比較している．グラフの結果が示しているように，時間の経過とともに実際の転送数とプロミスキャスモードで捕捉した転送数のズレが拡大していくことが分かる．その結果図 6 で示しているように，隣接ノードに対するノード信頼度は時間の経過とともに約 0.6(紫線) に収束していくことが分かる．それに，パケット破棄率を 20%，33%，50% に設定して攻撃した場合でも，実際にパケット破棄率より信頼度が低く精度が悪いことが分かる．

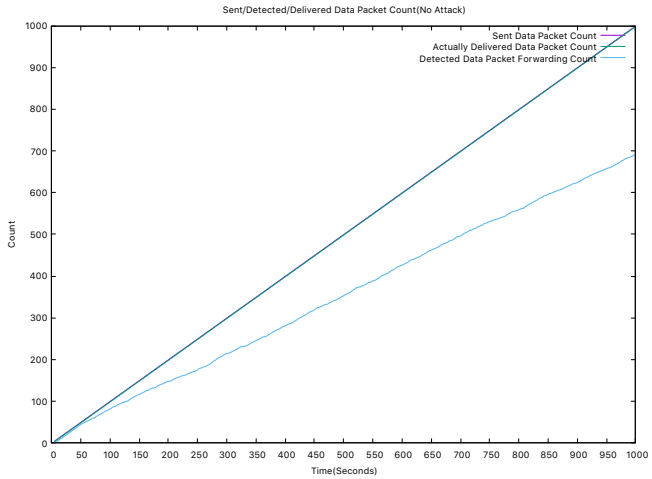

図 3　実際の転送数と捕捉した転送数のズレ

3.　提案手法

3.1　提案手法の概要

本稿では各 TrustRecordListEntry に TrustModelTrainer(3.4 で説明) を導入してノード信頼度の評価モデルを通信環境に合わせて訓練し，ノード信頼度を補正することによって信頼度評価の精度を向上させる手法を提案する．TrustRecordListEntry が生成されてから RUFB パケット (3.3 で説明) のやり取りや TrustModelTrainer によるモデル訓練までの流れは図 4 に示す．

表 1　各種パラメータ

TrainingPeriod	モデルの訓練周期
RouteFeedbackRequestPeriod	RUFB Request の送信周期
MinimumCountRequirement	訓練用入力データの基準数
LearningRate	環境変数と重みの学習率
Epoch	学習回数
Tolerance	ノード信頼度の許容誤差

各 TrustRecordListEntry は専用の TrustModelTrainer とつながっており，そのエントリが管理する隣接ノードとの通

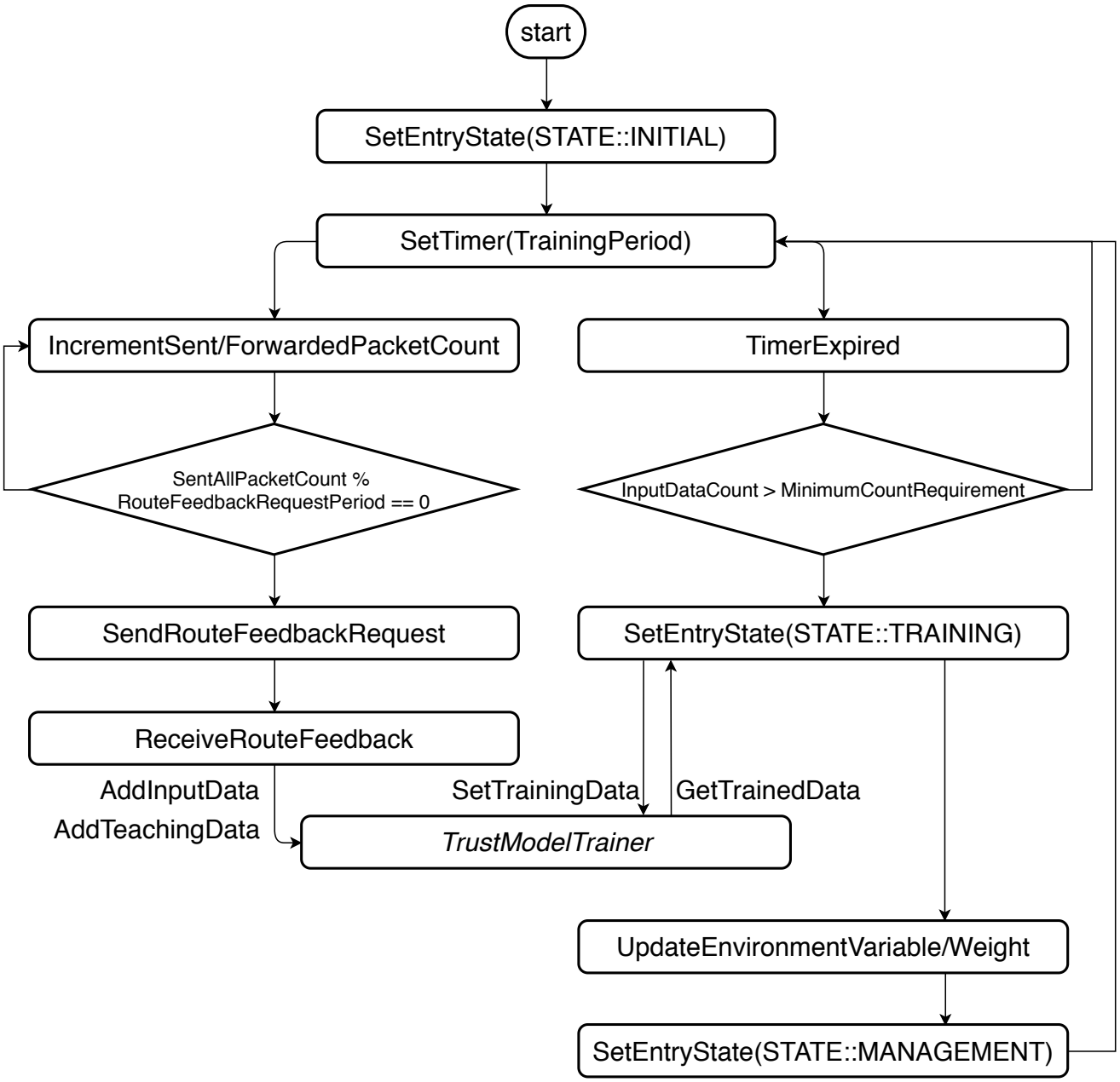

図 4 TrustRecordListEntry

信環境に合わせてモデルを訓練する．訓練に関する設定を行うためのパラメータは表 1 に示す．

3.2 ノード信頼度モデル

$$T_{jk}(t) = \omega_{CFR} \times E_{CFR} \times CFR_{jk}(t) + \omega_{DFR} \times E_{DFR} \times DFR_{jk}(t) \quad (4)$$

提案手法では既存のノード信頼度モデルに環境変数として E_{CFR}, E_{DFR} を追加する．そして TrustModelTrainer では重み (ω_{CFR}，ω_{DFR}) と環境変数 (E_{CFR}，E_{DFR}) を訓練する．環境変数の初期値は 1 であり，機械学習により修正され $CFR_{jk}(t)$ と $DFR_{jk}(t)$ を補正する．ω_{CFR}，ω_{DFR} は重み定数であり，送信したパケットの総数に対する割合に合わせて調整される．

3.3 Route Feedback(RUFB)

提案手法では訓練で使用する教師データを確保する手段として，新たな制御パケットである RouteFeedback(RUFB) パケットを導入する．RUFB パケットは隣接ノードからリクエスト (RouteFeedbackRequest) が届いた場合に限り送信し，リクエストを送信してきたノードから実際に受信した制御パケット数とデータパケットの数をフィードバックする．RouteFeedbackRequest は事前に設定した RouteFeedbackRequestPeriod ごとに自動的に送信され，受信した情報は TrustModelTrainer の入力データ (InputData) として追加される．

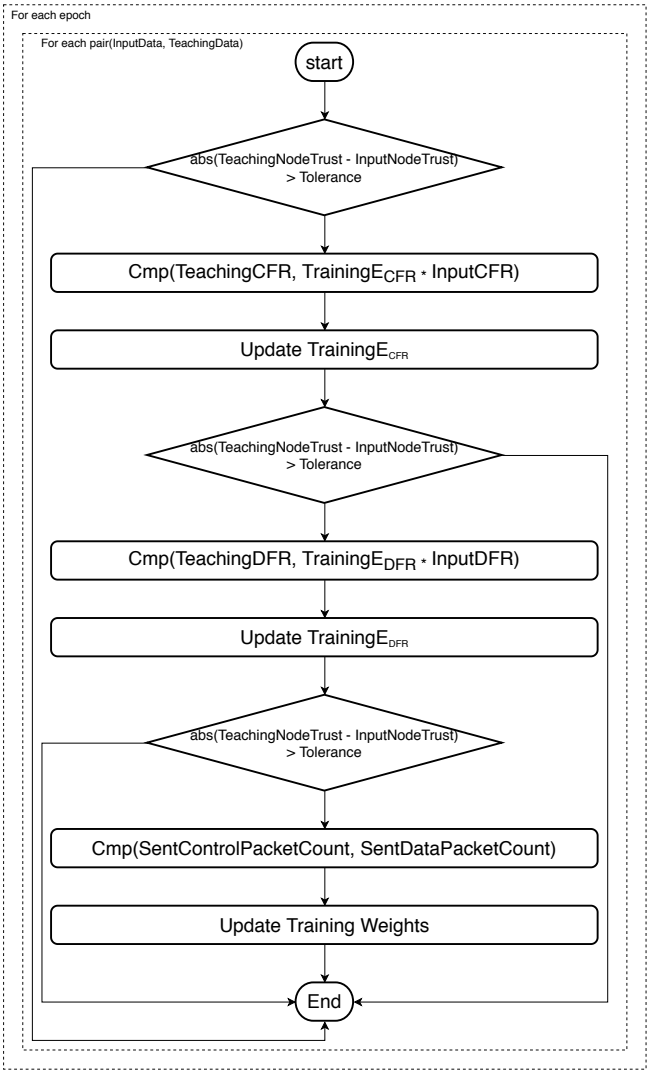

図 5 TrustModelTrainer

3.4 TrustModelTrainer

TrustModelTrainer は各 TrustRecordListEntry におけるノード信頼度モデルを訓練する．訓練条件が充足したら蓄積された教師データ (TeachingData) と入力データ (InputData) のペアを順番に呼び出してノード信頼度の教師データを実際計算したデータを算出する．そして事前に設定した許容誤差との比較を行い，その誤差を超えた場合は環境変数から重みまでの順で学習していく．提案手法では精密な調整を行うため，ノード信頼度モデルの全パラメータを同時に変化せず，個別に調整を行う．TrustModelTrainer における訓練の流れは図５で示す．

CFR と DFR の教師データは，RUFB パケットによって受信した制御パケット数とデータパケット数を送信したパケット数と比較して算出する．この教師データを InputData として入力された CFR と DFR に環境変数 E_{CFR} と E_{DFR} をかけた値を比較し，教師データに近似させる方向に各環境変数を学習率 (LearningRate) の分増減させる．

重み ω_{CFR} と ω_{DFR} は制御パケットとデータパケットの送信数を比較し，送信数が多い側の重みを学習率の分増加させ，もう一方の重みを同じ学習率の分減少させる．環境変数は CFR と DFR のズレを埋め合わせる役割をするが，重みは制御パケットとデータパケットの割合を考慮するためである．以上４つのパラメータをそれぞれ調整することにより，訓練の精度を高めることができる．

3.5 TrustRecordListEntry

TrustRecordListEntry は３つの状態 (State) を持っている．最初エントリが生成したときは INITIAL 状態で，訓練周期の分タイマーを設定する．その後，最初にモデル訓練するときに INITIAL 状態から TRAINING 状態に移行し，訓練が終わったら MANAGEMENT 状態に移行した後，TRAINING と MANAGEMENT 状態を交互に移行する．INITIAL 状態のときはまだ周りの環境に合わせてノード信頼度モデルを訓練してないため，この状態で算出したノード信頼度は 1 に反映する．計算したノード信頼度によるルーティングは最初に MANAGEMENT になってから行う．

4. シミュレーション評価

提案手法の有効性を示すため，ns-3(network simulator 3)[10] で評価を行い，任意のノードにおけるノード信頼度とノード信頼度モデルのパラメータの変移を確認し，既存手法におけるノード信頼度の精度問題が改善されたことを確認した．

4.1 シミュレーション構成

シミュレーションに関する各種パラメータ設定内容を表２に示す．

表 2 シミュレーション構成

network simulator	ns-3.30
simulation time：t	1200s
number of nodes	50
map size	1000m x 1000m
mobility model	constant position
traffic type	constant bit rate(CBR)/UDP
transmission radius	250m
packet size	1024 bytes
connection rate	1 pkts/s
initial E_{CFR}	1
initial E_{DFR}	1
initial ω_{CFR}	0.2
initial ω_{DFR}	0.8
training epoch	30
packet drop rate	20%，33%，50%
learning rate	0.01
route feedback request period	10 packets
training period	50s
minimum count requirement	10
tolerance	0.01

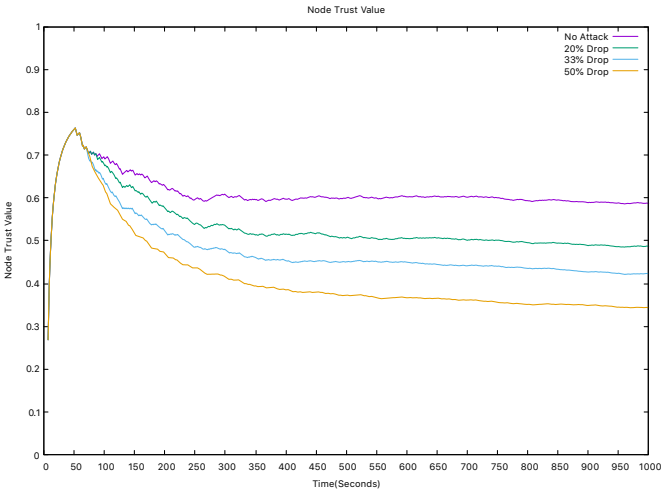

図 6　既存手法におけるノード信頼度の変化

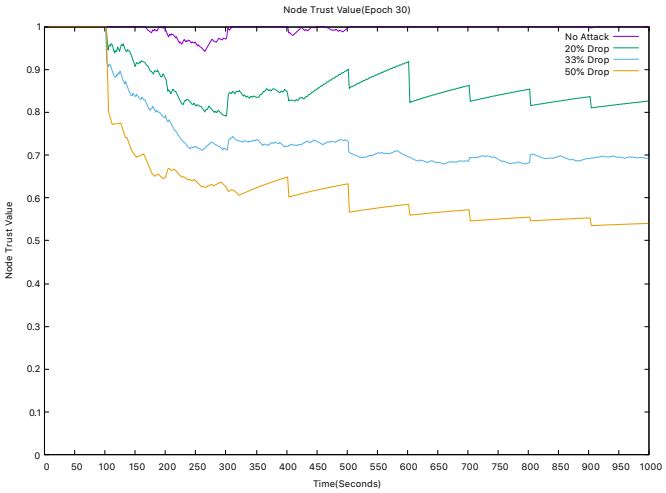

図 7　提案手法におけるノード信頼度の変化 (Epoch 30)

4.2　シミュレーション結果

シミュレーション評価を行った結果，図 6 と図 7 で示しているように，提案手法を適用する前は様々な要因によりノード信頼度が実際のノード信頼度と約 0.4 程度の大きな差を見せたが，提案手法で補正したノード信頼度が実際のノード信頼度にほぼ一致することを確認した．特にパケット破棄率を変化しながら攻撃した場合も，それに合わせて正しくノード信頼度を評価することを確認した．図 7 のグラフの線が滑らかでないのは，一定周期ごとに補正を行う行動と，補正した後も時間の経過とともに実際のパケット転送数と捕捉したパケット転送数のズレが拡大する現象が繰り返されるためである．これらの問題は訓練回数 (Epoch) や訓練周期 (TrainingPeriod)，訓練データの基準数 (MinimumCountRequirement) を調整することにより補完できる．

図 8 と図 9 は TrustModelTrainer により，時間の経過とともに環境変数 E_{CFR} と E_{DFR} が動的に変化していく様子を示しており，図 10 と図 11 は重み ω_{CFR} と ω_{DFR} が変化していく様子を示している．今回のシミュレーション実験では，実際の制御パケット数と捕捉して制御パケット数のズレが大きく，全体の送信数も少なかったので，E_{CFR} の値が初期値 1 から最大 7 まで増加した．E_{DFR} は最初は，E_{CFR} よりはそれほど変化してなく，33% パケット破棄攻撃の場合を除いては，時間の経過とともに初期値のほうに戻ってくることを確認した．そしてデータパケットが制御パケットより圧倒的に多かったため，シミュレーション時間 100 秒の時点で ω_{CFR} はほぼ 0 に，ω_{DFR} はほぼ 1 に近似した．

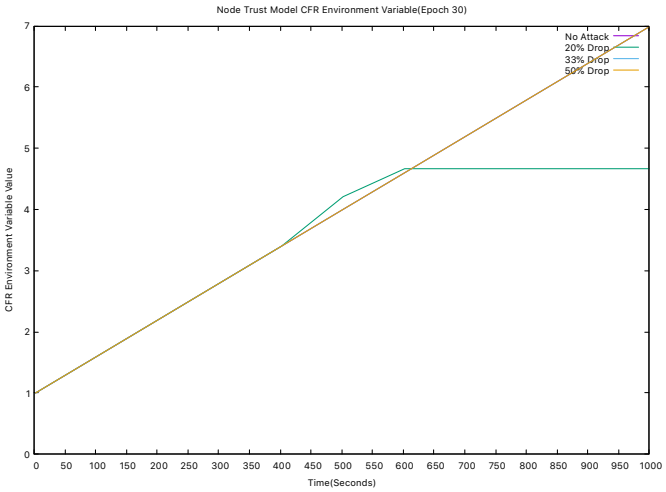

図 8　提案手法における環境変数 E_{CFR} の変化 (Epoch 30)

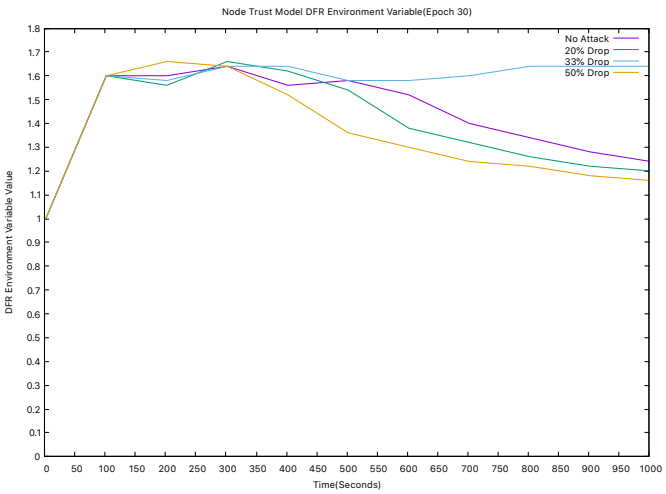

図 9　提案手法における環境変数 E_{DFR} の変化 (Epoch 30)

5.　結論

本稿では，ネットワーク混雑による衝突，受信バッファのストレージ不足，弱い電波強度，移動性による一時的な通信範囲離脱など，原因を特定することが難しい様々な要因を，環境変数と重みを訓練することにより，まとめて能動的に対応できる手法を提案した．今後は RUFB リクエストに対してウソをつくなど，様々な攻撃形態に対する対策を研究するとともに，状況による訓練の優先順位修正や学

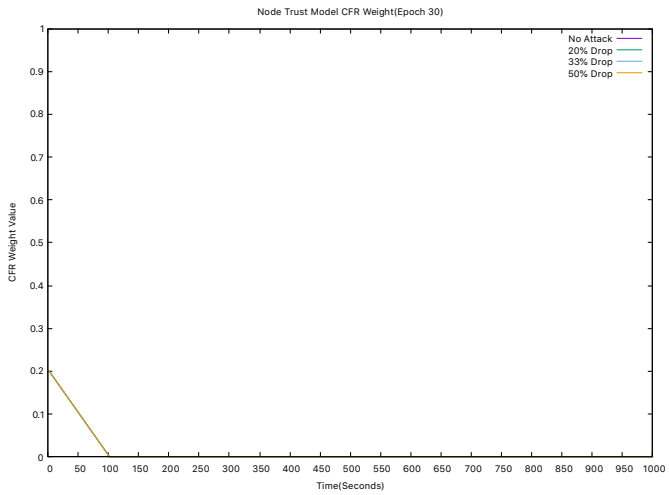

図 10 提案手法における ω_{CFR} の変化 (Epoch 30)

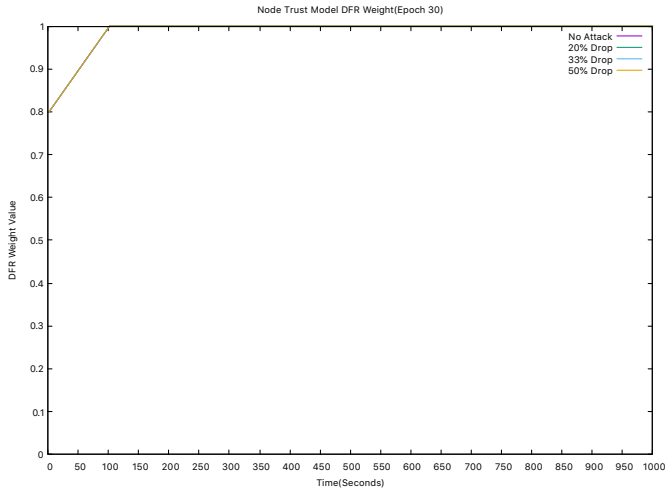

図 11 提案手法における ω_{DFR} の変化 (Epoch 30)

習率の動的変化などによってさらに精度を向上させる方法を研究していく.

参考文献

[1] Corson.S, Macket.J: *Mobile Ad hoc Networking(MANET): Routing Protocol Performance Issues and Evaluation Considerations*, RFC 2501, Informational, 1999

[2] Shuaishuai Tan, Xiaoping Li, Qingkuan Dong: *A Trust Management System for Securing Data Plane of Ad-Hoc Networks* IEEETransactions on vehicular technology, Vol.65, No.9, 2016

[3] Marti S., Giuli T., Lai K., Baker M.: *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*, Proc. Int. Conf. Mobile Computing and Networking (MobiCom), 2000, pp.255-265

[4] 藤田 毅: *C++*で学ぶディープラーニング, 株式会社マイナビ出版

[5] Pirzada A.A., Mcdonald C., Datta A.: *Performance Comparison of Trust-Based Reactive Routing Protocols*, IEEE trans. Mob. Comput, 2006, pp.695-710

[6] X.Li, Z.jia, P.Zhang, R.Zhang, H.Wang: *Trust-Based On-Demand Multipath Routing in Mobile Ad Hoc Networks*, IET Information Security, 2010.

[7] Sun Y., Yu W., Han Z., Liu K.J.R.: *Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks*, IEEE J. Sel. Areas Commun., 2006, (2), pp.305-317

[8] Farruh Ishmanov, Yousaf Bin Zikria: Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issue

[9] 牛窪 洋貴, 武田 苑子, 重野 寛: モバイルアドホックネットワークにおけるトラストを利用した効率的セキュアルーティング, 情報処理学会論文誌, Vol.55, No.2, 2014, pp.649-658

[10] *ns-3: ns-3-manual*, https://www.nsnam.org/documentation, 2019